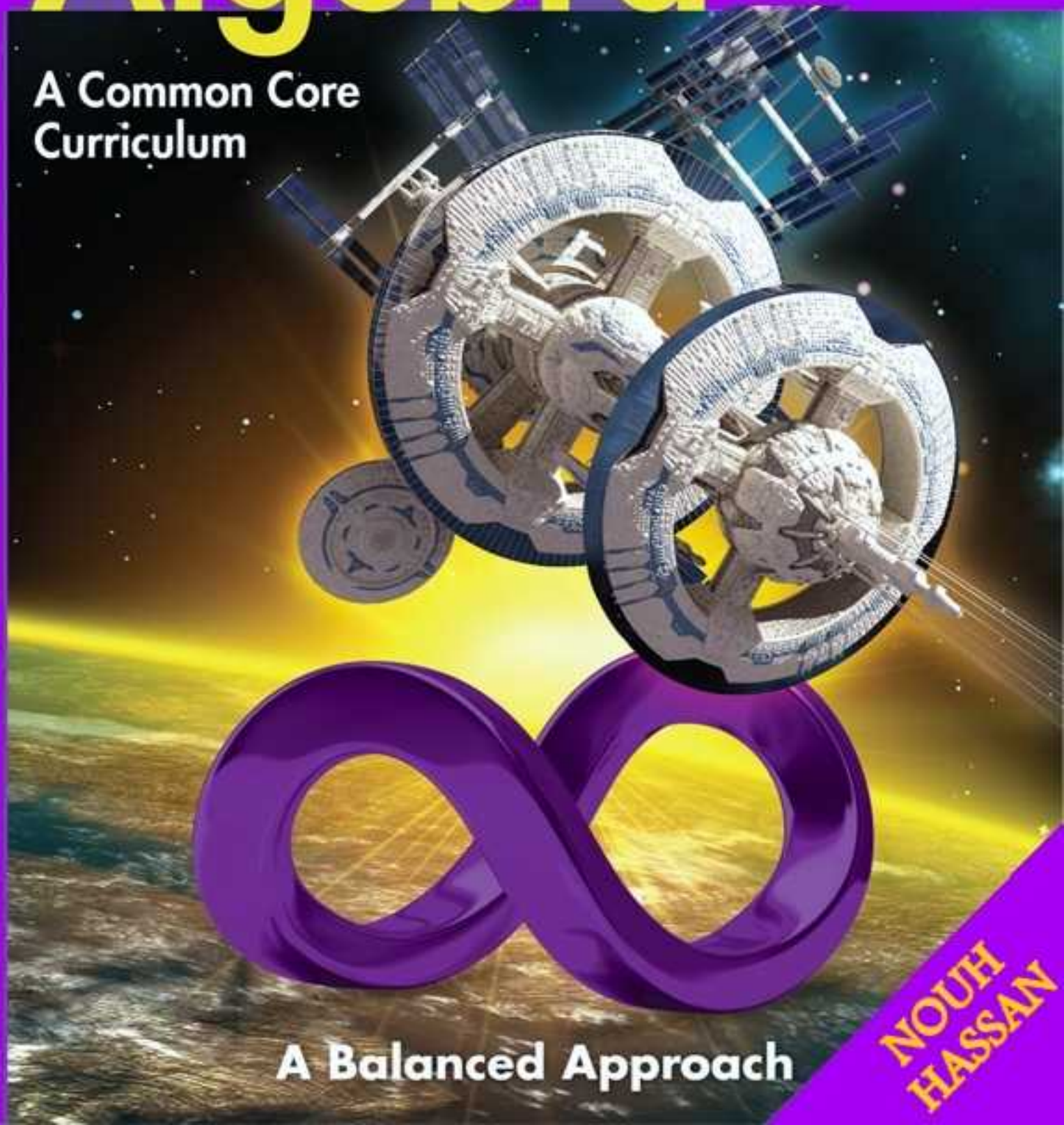
MATHEMATICS

Algebra

A Common Core Curriculum



A Balanced Approach

NOUH HASSAN

Pure Mathematical Physics

All rights are reserved

Translated by:

Diab Publishing & Distribution

www.Diab-publishing.com

Preface

This book contains valuable lessons of scientific value in mathematics, especially in relation to the wide field of sports (Algebra).

This book is the unique encyclopedia of mathematics that helps in the teaching profession and in the culture of mathematics and in the contemporary aspects of this book with the various sciences of physics, engineering and technical sciences.

Since childhood I got accustomed to study with a pen in my hand.

I extracted theorems and formulas, together with the definitions, from my text books.

It was easier, later, for me, to prepare for the tests, especially for the final exams at the end of the semester.

I kept (and still do today) small notebooks where I collected not only mathematical but any idea I read in various domains.

Besides the textbooks I added information I collected from various mathematical books of solved problems I was studying at that time.

This book contines the following chapters which are: Arithmetic, Plane Geometry, and Space Geometry, Algebra (9th to 12th grades), Trigonometry and Field and Galois theory.

The researcher Mr. Nouh Hassan has relied on special curricula for educational education, research education and mathematics. It is a riches for the pioneers of mathematics and the world of the comprehensive scientific level.

Author Nouh Hassan

17/11/2019

Mr. Nouh Hassan in brief:

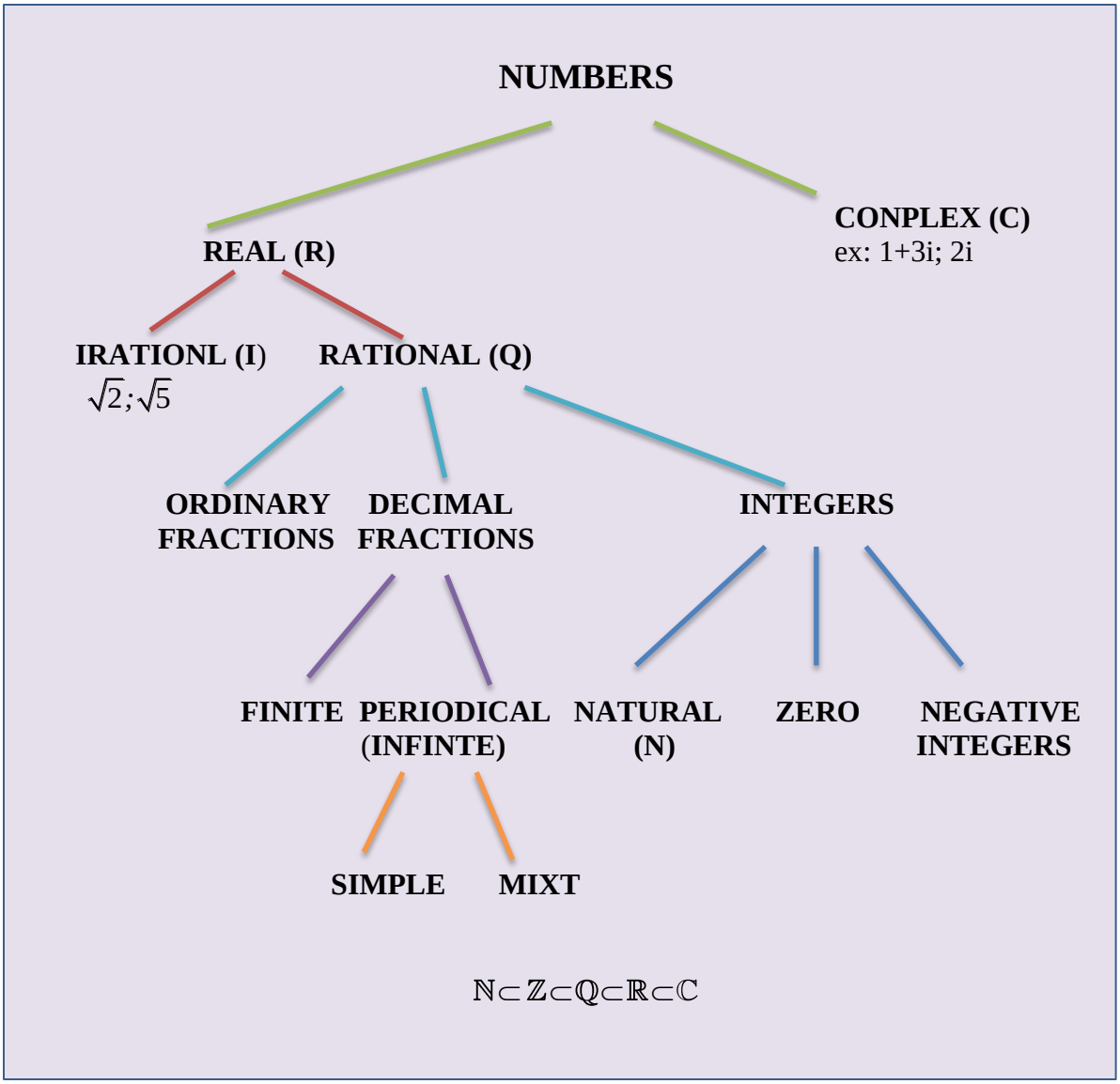
- Born in 1957, Maarake Village, Tyre in southern Lebanon.
- He received his primary and intermediate education at the official battle school and finished high school at the official secondary school.
- He graduated from the Teachers' and Teachers' College in Nabatieh in 1979.
- He obtained his educational leave from the Lebanese University in mathematics in 1985.
- He was ranked first in Mathematics in the Lebanese Civil Service Council in 1995.
- He completed his graduation from the Faculty of Education at the Lebanese University in 1996 with the rank of secondary professor in the staff of the Ministry of National Education.
- Participated in many educational activities, training courses and public events.

Contents

1. Arithmetic……...…1
2. Plane Geometry……..…34
3. Space Geometry…….....80
4. Algebra (9thto 12th grades)……..…...111
5. Trigonometry……..…179
6. Field and Galois theory……...…212

Chapter One:

□ rith□ eti□



Numbers

- Ordinary (shows the order of elements; first, second, etc.)
- Cardinal (shows how many elements are in a set; seven, six, etc.)

Numbers:

- Concrete (when it is specified the nature of the counted elements: 14 apples)
- Abstract (when there is no specification of the elements: 14, 3, 100, etc.)

Systems of numeracy

a) Primitive numeration
   - The numbers are written with lines I; II, III, IIII, IIIII
   - Are connected with the fingers from the hand

b) Using the letters (Romans)

I V X L C D M

1 5 10 50 100 500 1000

For numbers larger than four thousands it is indicated the number of the thousands by the letter m or we put above the number indicating the thousands a line:

XXIMDCXII = 21,612

IVC = 4100

$\overline{\overline{XI}}\ \overline{CDX}\ DC$ =11,410,600

Numeration systems in the decimal base

- The digits: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0 (ten digits)
- In a number a digit shows two things:
  - Through the position where it is written shows the group to which it belongs;
  - Through its value its shows how many groups are there.

Positional system

Definition

The positional system is the numeration system in which through the place where it is written a digit, indicates the type of the group.

In a numeration system with the base B there is the need of B digits from 1 to $B-1$ and the digit 0 (zero). The grouping is done in B units. B units of one order form a unit of a superior order.

Dozen is a group of 12 units.

The Babylonians used the base 60; from those times it remained the division of the hour or the degrees, as 60 minutes in an hour, and the minute in 60 seconds.

Transformation of a number from a given base to another base

Transformation of a number from a given base to base 10.

$$0.234_{(5)} = \frac{2}{5^1} + \frac{3}{5^2} + \frac{4}{5^3}$$

$$6053_{(8)} = 6\cdot 8^3 + 0\cdot 8^2 + 5\cdot 8^1 + 3 = 3115_{(10)}$$

Transformation of a number from base 10 to another base

$$1253_{(10)} = N_{(7)} = 3440_{(7)}$$

Successive divisions

1253	7
55	179
63	39
0	4

7	
7	
25	7
4	3

Transformation of a number from a random base to another base different of 10

The number will be transformed first in base 10 and then in the required base.

Addition

Definition

The addition is a binary operation in which to any pair (ordered) of elements of a set corresponds one element of the same set.

$a+b=c$

a,b - Addition terms

c - The result of the sum (total)

Properties of Additions

1) Commutability $a+b=b+a$. There exists an element neutral such that $a+0=a$
2) Associativity $(a+b)+c=a+(b+c)$

The sum of numbers written in other bases

$$\begin{array}{r} 8756_{(9)} \\ +2045_{(9)} \\ \hline 11812_{(9)} \end{array}$$

During the sum it must be taken into consideration that the numbers should have the same measure.

Subtraction

The operation of subtraction is the invers operation of addition.

$a-b=c$

a,b The subtraction's terms: (a is called the minuend, b is called the subtrahend)

c is called the difference

Properties of subtraction

1) If the minuend is increased (or diminished) with a number, the difference increases (or diminishes) with the same number.
2) If the subtrahend is increased (or decreased) with a number, the difference decreases (or increases) with the same number.
3) If both terms of a subtraction are increased (or decreased) by the same number, the difference will not change.
4) To subtract a number from a sum it is sufficient to subtract it from one of the terms of the sum.

The subtraction in a given positional number system

$$\begin{array}{r} 28504_{(9)} \\ -\ 3615_{(9)} \\ \hline 24778_{(9)} \end{array}$$

Definition

The arithmetic the complement of a number, which does not end in zero, is the difference between the power of 10 that is immediately superior to that number.

Multiplication

To multiply a number with another number it means to repeat adding this number as many times shown in the second number. The multiplication is a repeated addition

$a \cdot b = c$

a,b Are called the multiplication's factors

c Is called the product

a Is called the multiplicand

b Is called the multiplier

The properties of multiplication

1) Commutative: $a \cdot b = b \cdot a$
2) Associative $(a \cdot b) \cdot c = (a \cdot b) \cdot c$
3) Distributive with respect to addition $a \cdot (b + c) = ab + ac$

To multiply a number with a product, we'll multiply the number with a factor of the product.

If a factor of the product increases (or diminishes) m times, then the product itself increases (or diminishes) by the same number of times.

The multiplication of the numbers written in a given positional number system

$$\begin{array}{r} 234_{(5)} \\ \cdot 402_{(5)} \\ \hline 1023 \\ 2101 \\ \hline 211123_{(5)} \end{array}$$

The number of the digits of a product

If the number a has m digits and the number b has n digits, then the product $a \cdot b$ has $m+n-1$ or $m+n$ digits.

Division

Division is the inverse operation to multiplication.

The division can be exact ($r = 0$), or with reminder $0 < r < divisor$

The properties of division

1) To divide a product by a number it is sufficient to divide by that number only one of the product's factors.
2) If we multiply the dividend and the divisor by the same number, the quotient doesn't change.
3) If we divide the dividend and the divisor by the same number, the quotient doesn't change.
4) To divide a number by a product, we'll divide each factor of the product by that number.

$$\frac{a}{b} = c$$

a Is called the dividend
b Is called the divisor
c Is called the quotient

To divide a sum or a difference by a number, we'll divide each term of the sum or difference by that number.

$$\frac{a+b+c}{m} = \frac{a}{m} + \frac{b}{m} + \frac{c}{m} \text{ or } \frac{a-b-c}{m} = \frac{a}{m} - \frac{b}{m} - \frac{c}{m}$$

If the dividend increases (or diminishes) by a number, the quotient will increase (or decrease) by the same number.

$$\frac{a}{b} = q;\ \frac{a}{b \cdot m} = \frac{q}{m};\ \frac{a}{\frac{b}{m}} = qm$$

Division with remainder

$$a = b \cdot q + r,\ r < b$$

If we divide the dividend and the divisor by the same number, the quotient doesn't change, but the remainder is divided by that number.

Partial remainders

$$\begin{array}{rl|l} 4847 & & 23 \\ \underline{46} & & \overline{210} \\ R_1 = 24 & & \\ \underline{23} & & \\ R_2 = 17 & & \\ R_3 & & \end{array}$$

R_1 =2 is the partial remainder

R_2 =1 is the partial remainder

R_3 =17 is the final reminder

Algorithm

Definition

An algorithm is a method that consists of a succession of computations, all fallowing the same process.

For example: the Euclid's algorithm, the division is also called the division algorithm.

Measuring quantities

The fundamental measures: length, mass, time. The fundamental units of measurement: meter, gram, second.

Derived measures: speed, area, etc.

Etalon meter is a meter build from platinum, which is kept in Paris (is length is constant).

The prefixes used in the multiples and submultiples of certain units:

Kilo

Hecto

Deka

Meter

Deci

Centi

Mili

Debit = capacity/time

Norm= quantity/time

Ratio=quantity/time

Density=mass/volume $\varphi = \frac{m}{V}$

Acceleration = $\frac{v_2 - v_1}{t}$

Relation between three fundamental units: 1 liter-1 kg= $1dm^3$

Arithmetic mean

$$a = \frac{a_1 + a_2 + ... + a_n}{n}$$

$a_k - a$ = deviation in plus with respect to the mean

$a - a_k$ = deviation in minus with respect to the mean

$1 \le k \le n$

The sum of deviations in plus is equal to the sum of deviations in minus.

Another mode to compute the arithmetic mean

Let the numbers 200, 260, 290. These numbers can be written as 200, 200, 200 + 60+90;

$$\frac{60+90}{3}=50;\ 200+50=250$$

Properties of arithmetic's mean

1) The arithmetic average is contained between the smaller and the largest given values, it is said that it is internal.
2) If one of the given values increases and then the average increases; it is said that the arithmetic average is monotone. If a_1 increases by h, then he average grows by $\frac{h}{n}$.
3) If we substitute two or more of the given values by their partial average, the general average does not change, it is said that the arithmetic average is associative.

$$\frac{a_1+a_2+...+a_n}{n}=\frac{a'+a'+a'+a_4+...+a_n}{n}$$

$$\frac{a_1+a_2+a_3}{3}=a'\Rightarrow a_1+a_2+a_3=a'+a'+a'$$

4) If all given values increase by the same number h and the arithmetic average grows also by h; it is said that the arithmetic average is translated.
5) If all given values are multiplied by the same number h the arithmetic average is multiplied by h; it is said that the arithmetic average is an homogenous function of first degree in the given values.
6) The amount of deviation from the mean is zero.

The square of deviations

$$(a_1-A)^2+...+(a_n-A)^2=a_1{}^2+...+2naA+nA^2=a_1{}^2+...+a_n{}^2-na^2+n(a-A)^2$$

The deviations square with respect to a number A is minim when this number is the arithmetic mean ($A=a$).

Pondered average

$$a=\frac{a_1k_1+a_2k_2+...+a_nk_n}{k_1+k_2+...+k_n}$$

The pondered average has the same properties as the arithmetic average

The ratio of mixed quantities is inversely equal to the ratio between the averages deviations:

$$\frac{k_2}{k_1}=\frac{t-t_1}{t_2-t}$$

Problems of mixtures and alloy

1) The concentration of a solution
2) The title of an alloy
3) Caloric balance

Geometric mean

$$\frac{x}{a}=\frac{b}{x}\Rightarrow x^2=ab\Rightarrow x=\sqrt{ab}$$

Harmonic mean

$$\frac{2}{x}=\frac{1}{a}+\frac{1}{b}\Leftrightarrow x=\frac{2ab}{a+b}$$

Methods of solving arithmetic problems

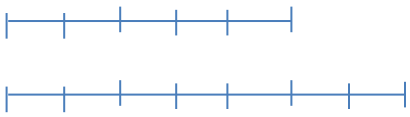
a) Algebraic
b) Through arithmetic rational

The figurative method

The figurative method consists in representing, through a design, the unknown elements, and by fixing into the design the relations between the elements or the relations between the given elements and the quantities given by the problem.

Example 1

A container has $\frac{7}{5}$ more water than another container, and together the containers have 240 liters. How many liters have each container?



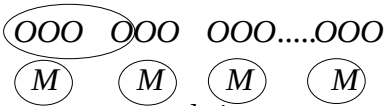
First container = 5 parts

Second container has 7 parts

5 parts +7 parts = 12 parts (both containers)
120 liters ÷ 12 parts = 20 liters each part
20 liters × 5 = 100 liters in the first container
20 liters × 7 = 140 liters in the second container.

Example 2

In a basket with fruits are three times more oranges than apples. At the table are four people; each person takes one orange and an apple. In the basket remained four times more oranges than apples. How many oranges and how many apples were in the basket at the beginning?



At the table were consumed 4 oranges and 4 apples. There remained 3 + 3 + 2 = 8 oranges (from the 4 groups, and 0 apples (4 – 4 = 0)); these are added to the 8 groups formed at the beginning (because the oranges have to be 4 times more).

8 group + 4 groups = 12 groups (initially)

$12 \times 1 = 12$ apples
$12 \times 3 = 36$ oranges

Types of problems

1) Find two numbers knowing their sum and their difference.
2) Find two numbers knowing their sum and their ratio.
3) Find two numbers knowing their difference and their ratio.
4) Problems of elimination of an unknown through sum and difference.

The method of reduction to the same comparative term

This method derives from resolving a system through the method of reduction.

Example

For 9 meters of fabric and 5 meters of silk one person spent $1,950.00. For 3 meters of fabric and 7 meters of silk (same qualities) one spent $1,290.00. How much cost 1 meter of fabric and how much cost 1 meter of silk?

9 m fabric…….5 m silk……$1,950.00
9 m fabric…….7 m silk……$1,290.00/$\times 3$

---

9 m fabric…….5 m silk……$1,950.00
9 m fabric……21 m silk……$3,870.00

/ 16 m silk……$.1,950.00

……..1m silk = $\frac{\$1,920.00}{16m} = \$120/m$ silk

$120.00/m $\times$ 5 m = $600.00

…$1,950.00 - $600.00 = $1,350 – the cost of 9 m of fabric

$1,350.00 $\div$ 9 m = $150.00/m fabric.

The method of the false hypothesis

Problem

There are 100 glasses, some have the capacity of 20 cl, and others have the capacity of 35 cl. If all glasses are filled, the total quantity of liquid will be 2,870 cl. How many glasses of each kind are there?

We suppose that we fill up only the glasses with the capacity of 20 cl:
$20 \text{ cl} \times 100 = 2{,}000$ cl.
The liquid left is: 2,870 cl -2,000 cl = 870 cl
The small glasses are now all full.
35 cl – 20 cl = 15 cl
The quantity of liquid left has to be added to the larger glasses.
$870 \div 15 = 58$ large glasses
100 glasses – 58 large glasses = 42 small glasses.

The method of resolving by starting from the end to the beginning of a problem

The problems are resolved from the end to the beginning.

Example

A number is selected; it is multiplied by 5. To the result is added 42, the sum obtained is divided by 7, and from the quotient it will be subtracted 11, obtaining 200. What is the selected number?

$(x \cdot 5 + 42) \div 7 - 11 = 200$

- Which is the last operation? "from the quotient subtract 11 to obtain 200"; 200+11=211
- "The sum obtained has been divided by 7 and it has been obtained 211"; 211×7=1477"
- We added 42 and we obtained 1477"
- 1477-42=1435
- "A number multiplied by 5 gives 1435"
- 1435 ÷ 5 = 287; this is the selected number.

Combined problems

Are used several methods: a complex problem is decomposed in a couple of simple problems; it is used a process of creative, progressive thinking.

Divisibility of the natural numbers

$a \vdots b$ (a is divisible by b)

$b \mid a$ (b divides a)

The set of multiples of a number

$M_a(0;a;2a;3a;...ia;...)$

The set of the divisors of a number

$D_{24} = \{1,2,3,4,6,8,12,24\}$

The set of the common divisors of two numbers is the set of the divisors of those two numbers

Two or more numbers which don't have a common divisor besides 1 are called prime numbers between them $(a,b)=1$, example $(10,21)=1$.

The set of the common divisors of n numbers is the set of the common divisors of those numbers.

Three numbers are prime between them if $(a,b,c)=1$.

The numbers are prime between them two by two if $(a,b)=1;(b,c)=1;(c,a)=1$.

The rules of divisibility

1) The sum (difference) of several multiples of a number is itself a multiple of that number.
2) The sum of several numbers, some multiples of b, others which give a reminder different of zero, when divided by b, is a multiple of b only when the sum of reminders is a multiple of b.

3) If two numbers a,a' gives the same reminder when divided by b, then their difference is a multiple of b. In this case the numbers are called congruent modulo b $a \equiv a'(mod\, b)$

4) If a is a multiple of b, and b is a multiple of c, then a is a multiple of c.

Divisibility criteria

a) Divisibility by 2: A number is divisible by 2 if its last digit is zero or is divisible by 2 (0,2,4,6,8).

b) Divisibility by 5: A number is divisible by 5 if its last digit is zero or 5.

c) Divisibility by 4: A number is divisible by 4 if its last two digits are divisible by 4.

d) Divisibility by 25: A number is divisible by 25 if its last two digits are divisible by 25. (the last two digits are 00, 25,50, 75, etc.)

e) Divisibility by 8: A number is divisible by 8 if its last three digits are divisible by 8.

f) Divisibility by 125: A number is divisible by 125 if its last three digits are divisible by 125.

g) Divisibility by 3: A number is divisible by 3 if the sum of its digits is a multiple of 3.

h) Divisibility by 9: A number is divisible by 9 if the sum of its digits is a multiple of 9.

i) Divisibility by 11: A number is divisible by 11 if and only if the difference between the sum of its digits, located on even places and the sum of its digits, located on odd places is a multiple of 11. Example: 76.035

$$S_1 = 5+0+7 = 12$$
$$S_2 = 3+6 = 9$$
; $76035 = \circlearrowright\!\!\!\!\!\!M 11 + S_1 - S_2 = \circlearrowright\!\!\!\!\!\!M 11 + 12 - 9 = \circlearrowright\!\!\!\!\!\!M 11 + 3$

j) Divisibility by 7: A number is divisible by 7 if the difference between the sum of classes of odd order and the sum of the classes of even order is a multiple of 7. Example 72.813.605

$$S_1 = 606 + 72 = 677$$
$$S_2 = 813$$
$$72.813.605 = \circlearrowright\!\!\!\!\!\!M 7 + S_1 - S_2 = \circlearrowright\!\!\!\!\!\!M 7 + 677 - 813 = \circlearrowright\!\!\!\!\!\!M 7 + (136) = \circlearrowright\!\!\!\!\!\!M 7 - 3 = \circlearrowright\!\!\!\!\!\!M 7 + 4$$

k) Divisibility by 13: A number is divisible by 13 if the difference between the classes of odd order and the sum of the classes representing the even order is a multiple of 13. Example 81.670.200

$$S_1 = 200 + 81 = 281$$
$$S_2 = 670$$
$$81.670.200 = \circlearrowright\!\!\!\!\!\!M 13 + 281 - 670 = \circlearrowright\!\!\!\!\!\!M 13 - 389 = \circlearrowright\!\!\!\!\!\!M 13 - 12 = \circlearrowright\!\!\!\!\!\!M 13 + 1$$

l) The general criteria of divisibility:

Let

b the base of the numeration system

d the number for which we need to determine the divisibility criteria

r_i the remainders

Let $a = a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + ...a_1 \cdot b^1 + a_0$ the number for which we need to find the criteria to be divisible by d.

$$b^1 = \mathcal{C}d + r_1$$
$$b^2 = \mathcal{C}d + r_2$$
$$b^3 = \mathcal{C}d + r_3$$
.....
$$b^n = \mathcal{C}d + r_n$$
$$a = \mathcal{C}d + a_n r_n + a_{n-1} r_{n-1} + ... + a_1 r_1 + a_0$$

Theorems referring to Euclid's algorithm

Let a and b two natural numbers $a > b$, and $a = b \cdot q + r \ \ (r < b)$

1) If a number d divides b and r, then d divides also a;
2) If a number d divides a and b, it will divide also r;
3) If a number d divides a and r, then it will divide also b;
4) If $r = 0$, that is $a = b \cdot q$, then $(a,b) = b$ and $D_{a,b}$ = the divisors of b.

Euclid's algorithm (Euclidean Algorithm)

To find the greatest common divisor (GCD) of two given numbers a and b, $a > b$, we'll divide a by b, and we'll denote the remainder by r_1 that is $(a,b) = (b,r_1)$. We'll repeat the process with the numbers b and r_1, and so on, until will reach to a division of a remainder zero (assuming that there will be a finite number of operations).

The last's division's divider will be the GCD (the greatest common divisor) of he given numbers.

Example:

$(932,425)$

032=425x2+82
425=82x5+15
82=15x5+7
15=7x2+1
7=1x7

Therefore $(932,425) = 1$

Consequence of Euclid's algorithm

Any common divisor of two numbers divides the greatest common divisor of the given numbers.

$D_{a,b,c} = D_{a,b} \cap D_c$

To find the GCD of multiple numbers, we'll randomly group them, and find the GCD of each group, $d_1, d_2, ..., d_n$, then we'll determine the GDC of the $d_1, d_2, ..., d_n$.

Properties

1) If two given numbers are multiplied by the same number, then the GCD of the given numbers will be multiplied by the same number;
2) Let a and b two given numbers, whose one of the divisors is d. If a and b are divided by d, then the GCD will be divided by d. (If $(a,b)=D$, then $\left(\frac{a}{d},\frac{b}{d}\right)=\frac{D}{d}$;
3) The reminders of the division of two number by their GCD are prime numbers between them;
4) If a number divides a product of two numbers and it is prime with one of them, then it will divide also the other number in the product.

Common multiples

Theorems

1) $[a,b]=\frac{a\cdot b}{d}\left(=a_1\cdot b=a\cdot b_1\right)$.
2) The set of common multiples of two numbers is equal to the set of multiples of the least common multiple.
3) The least common multiple (LCM) of two prime numbers between them is the product of those numbers.
4) If a number n is divisible with each of the numbers a,b (prime between them), then it is also divisible with their product.
5) The quotient of LCM $[a,b]$ by the numbers a and b are two numbers prime between them.
6) $[a,b]=a_1\cdot b_1\cdot d$; $a=a_1\cdot d$ and $b=b_1\cdot d$
7) $\subset\mathcal{M}_{a,b,c}=\subset\mathcal{M}_{a,b}\bigcap\subset\mathcal{M}_c$

To find the LCM of several numbers we will form randomly selected groups. We'll determine the LCM of each group $m_1,m_2,...,m_n$, then we'll find the LCM of the groups formed from $m_1,m_2,...,m_n$, and so on.

Diophantine equations of first degree with two unknowns

This type of equations has been studied for the first time by the Greek mathematician Diophantus (IVth century)

General form $ax+by=c$, $(a,b)=1$; $(a,b,c)\in\mathbb{Z}$.

The computation of these equations is done in the set of integer numbers $x,y\in\mathbb{Z}$.

Example: Find the solution of the following equation $15x-26y=7$ in the set of integer numbers.

$$15x-26y=7\Rightarrow x=\frac{7+26y}{15}=y+\frac{7+11y}{15}$$

$$\frac{7+11y}{15}=p\Rightarrow 11y=15p-7$$

$$\frac{4p-7}{11}=s\Rightarrow p=\frac{11S+7}{4}=2S+1+\frac{3S+3}{4}\quad s\in\mathbb{Z}$$

$\frac{3S+3}{4}$ =r $\Rightarrow$ s= $\frac{3r-3}{3} = r-1+\frac{r}{3},\ r \in \mathbb{Z}$

$\frac{r}{3} = v \Rightarrow r = 3v,\ v \in \mathbb{Z}$,

Therefore, $r = 3v$; $r = 3v \Rightarrow s = 3v-1+v = 4v-1 \Rightarrow p = 8v-2+1+3v = 11v-1$

$\Rightarrow y = 11v-1+4v-1 = 15v-2$

$\Rightarrow x = 15v-2+11v-1 = 26v-3$.

The solutions are $\begin{cases} x = 26v-3 \\ y = 15v-2 \end{cases}\ v \in \mathbb{Z}$

There exists, therefore, an infinite pairs of solutions, which are obtained by giving to v different values $\{...,-2,-1,0,+1,+2,...\}$.

If we want that x and y to meet certain conditions, we'll form a system of inequalities giving to x and y the required conditions, and then determine the v values.

How is the method applied: We determine first the unknown with the smaller coefficient; extract the whole part from the ratio; the remaining ratio is denoted with a letter; the process is repeated until there is no ratio left. Then starting from the end we determine the values used in notations until the unknown x and y.

Theorems

1) Given the equation $ax = by + c$, where $(a,b) = 1$ and $0 < c < b$, through the numbers $x = 1,2,...,b$ exits one and only one number which verifies the equation; the corresponding value for y is less than a.
2) The solution for the equation $ax + by = c$ is given by the formula:

   $\begin{cases} x = x_1 + \lambda b \\ y = y_1 + \lambda a \end{cases}$ $\lambda \in \mathbb{Z}$; x_1, y_1 are a particular solution for the Diophantine equation.

The equation $ax + by = c$, where $(a,b) = d > 1$

Case I: If d divides also c, then the equation has solutions. The equation is divided by d, and then it is computed normal.

Case II: If d does not divide c, then the equation does not have solutions (it is called impossible).

Prime Numbers

- Divisors:
  a) Improper (1 and the number itself)
  b) Proper (divisors other than 1 and the number itself)
- Numbers
  a) Prime (don't have proper divisors)
  b) Composed (have proper divisors)

Number 1 is not prime or composed.

Theorem

The smaller divisor proper of a number is prime.

Properties of the divisors of a composed number

a) If b is a divisor whose square is bigger (smaller) than a, then $b_1 = \frac{a}{b}$ is a divisor whose square is smaller (bigger) than a.
b) The sequence of the prime numbers is infinite.

The sieve of Eratosthenes (III century BC)

Algorithm to find the sequence of prime numbers smaller than a given number a. It is a method of obtaining prime numbers by sifting out the composite numbers from the set of natural numbers so that only prime numbers remain.

In a table are written all number up to a.

Cross out all multiples of 2, starting with 2^2.

Then we cross out the multiples of 3, starting with 3^2.

Then we cross out the multiples of 5, staring with 5^2 and so on until we cross out $\mathcal{M}p$ starting with $\mathcal{M}p^2$, p prime. All numbers that remain in the table are prime.

Theorems

1) If a number a has a common divisor, which is a composed number b, then a has also a divisor prime smaller than b.
2) If a number does not have any divisor prime, ten it does not have any prime divisor composed number, then it will not have any divisor composed.

How to determine that a number is prime

Let a a given number, first will find the biggest prime number p which satisfies the condition $p^2 \le a$ and write all prime numbers until p; then we verify if each prime number it is a divisor for a.

If a is not divisible by any of these numbers, then a is a prime number.

Example:

Let consider the number 281, which is prime

We have $17^2 = 289 > 281$; we consider the numbers 2, 3, 5, 7, 11, 13. We verify that none of these numbers divides 281; therefore 281 is a prime number.

Decomposition of a number in prime factors

360	2
180	2
90	2
45	5
9	3^2
1	

therefore $360 = 2^3 \cdot 3^2 \cdot 5$

A number cannot have two distinct decompositions in prime factors.

Given two numbers A and B, decomposed in prime factors, the necessary and sufficient condition that A would divide B is that all prime factors of A can be found in the decomposition of B with the exponents at most equal.

The number of divisors of a number

Given a number

$$N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_n^{\alpha_n},$$

the number of its divisors is $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_n + 1)$.

To find the least common divisor of two or more numbers, each decomposed in factors, we'll consider the common factors with the smaller exponent.

To find the greatest common multiple of two or more numbers, each decomposed in factors, we'll consider the common ad not common factors at the greatest exponent.

$$[a,b] \times (a,b) = a \cdot b$$

Ordinary fractions

Sizes

- Commensurable (can be measured with a measurement unit)
- Incommensurable (cannot be measured)

$\frac{a}{b} = \frac{numerator}{deno\,min\,ator}$, a,b are called the fraction's terms

The fractions can be:

- Sub unitary fractions $\frac{3}{4}, \frac{7}{10}$ $(a < b)$
- Equi unitary fractions $\frac{1}{1}, \frac{5}{5}$ $(a = b)$
- Super unitary fractions $\frac{5}{4}, \frac{6}{2}$ $(a > b)$

Comparison of fractions

a) From two fractions, which have the same denominator, the bigger is that whose numerator is larger. $\frac{3}{4} > \frac{2}{4} > \frac{1}{4}$

b) From two fractions, which have the same numerator, the bigger is that whose denominator is smaller. $\frac{3}{2} > \frac{3}{3} > \frac{3}{4}$.

Amplification of fractions

To amplify a fraction means to multiply its numerator and denominator by the same number: $\frac{a}{b} = \frac{ma}{mb}$.

Simplification of a fraction

To simplify a fraction means to divide its numerator and denominator by the same number: $\frac{a}{b}=\frac{\frac{a}{m}}{\frac{b}{m}}$.

Solved problems

1) Prove that the greatest common divisor of the numbers $5n+3$ and $11n+8$ is 1 or 7. Find for what values of n the fraction $\frac{5n+3}{11n+8}$ can be simplified.

We'll denote $\begin{cases}A=5n+3\\B=11n+8\end{cases}$, if d divides A and B it will divide also:

$$11A+5B=\cancel{-55n}-33+\cancel{55n}+40=7,$$

therefore, d is 1 or 7 because $d\ /\ 7$, and $\frac{5n+3}{11n+8}$ can be simplified by 7.

$5n+3=\vdots 7$, therefore $5n=\vdots 7-3$, but $n=\vdots 7\pm k; 0\le k\le 6;\ k\in\mathbb{Z}$

a) $n=\vdots 7\Rightarrow 5n=\vdots 7\neq\vdots 7-3;$
b) $n=\vdots 7+1\Rightarrow 5n=\vdots 7+5\neq\vdots 7-3;$
c) $n=\vdots 7+2\Rightarrow 5n=\vdots 7+3\neq\vdots 7-3;$
d) $n=\vdots 7+3\Rightarrow 5n=\vdots 7+1\neq\vdots 7-3;$
e) $n=\vdots 7+4\Rightarrow 5n=\vdots 7+6\neq\vdots 7-3;$
f) $n=\vdots 7+5\Rightarrow 5n=\vdots 7+4\neq\vdots 7-3;$
g) $n=\vdots 7+6\Rightarrow 5n=\vdots 7+2\neq\vdots 7-3;$

therefore $n=\vdots 7+5=7k+5; k\in\mathbb{Z}$

2) Find for what values of a natural number n the fraction $\frac{5n+12}{2n+1}$ is an integer number.

We extract the integer part $\frac{5n+12}{2n+1}=\frac{4n+2+n+10}{2n+1}=2+\frac{n+10}{2n+1}$;

therefore $\frac{n+10}{2n+1}$ must be an integer.

Therefore $n+10\ge 2n+1\Rightarrow n\le 9$. We'll try one at the time all values of n, $n\in\{0,1,2,...,9\}$, and we find $n=9,\ n=0$.

If $\frac{a}{b}$ is not an integer, then $\frac{a^n}{b^n}$ is not an integer.

3) A boat rides on a river's watercourse with a speed of $14\frac{1}{2}Km$ per hour, and against the watercourse with a speed of 12Km per hour. What is the speed of the boat in stagnant water and what is the speed of the watercourse?

We denote v_1 the boat's speed in a still water and v_2 the speed of the moving water.

$$\begin{cases} 14\frac{1}{2}Km/h = v_1 + v_2 \\ 12Km/h = v_1 - v_2 \end{cases}$$

$$14\frac{1}{2} - 12 = 2\frac{1}{2} = \frac{5}{2}$$

$$\frac{5}{2} \div 2 = \frac{5}{4} Km/h = v_2$$

$$12 + \frac{5}{4} = 13\frac{1}{4} Km/h = v_1$$

Decimal fractions Decimal numbers)

In general, a decimal number is equal to a fraction which has as denominator the natural number, which we have in mind, when we delete the decimal point, and as numerator 10^n, n being the number of digits of the decimal part.

How to transform a decimal number to a number of another numeration bases

$$0.326_8 = 3\cdot 8^{-1} + 2\cdot 8^{-2} + 6\cdot 8^{-3} = \frac{3}{8} + \frac{2}{8^2} + \frac{6}{8^3} = \frac{326_8}{8^3}$$

The division can be

- Exact $(r = 0)$
- With reminder ($r \neq 0$ and $r <$ than the divider.

The quotient can be:

- Exact
- Approximate
  - In minus $\frac{4.7}{8} \approx 0.5$
  - In plus $\frac{4.7}{8} \approx 0.6$

The division of decimal numbers

$21.35 \div 4.3$

$$\begin{array}{r|l} 213500 & 43 \\ \hline 415 & 4.965 \\ \hline 280 & \\ \hline 220 & \\ \hline 5 & \end{array}$$

To find the remainders we'll write:

$213500 = 43\cdot 4.965 + 5 \;/\div 1000$

$213.5 = 43\cdot 4.965 + 0.005 /\div 10$

$21.35 = 4.3\cdot 4.965 + 0.0005$

Therefore, r=0.0005.

To divide two decimal numbers, we'll multiply the numerator and the denominator with 10^n, n being the number of decimals of the denominator. We are now in the case of the division of a decimal number (or whole) to an integer. In this way the quotient doesn't change; the remainder is multiplied also by 10^n.

Transformation of ordinary fractions in decimal fractions

The irreducible fraction $\frac{a}{b}$ is transformed in a decimal fraction finite id the numerator is of the form $2^{\alpha}\cdot 5^{\beta}$.

Simple periodical fractions

If $(b,10)=1$, the irreducible fraction $\frac{a}{b}$ can be transformed in a simple periodical fraction.

Mixed periodical functions

If the denominator b of a fractions of the form $b=2^{\alpha}\cdot 5^{\beta}\cdot b_1$, where b_1 is prime with 10, then $\frac{a}{b}$ is transformed in mixt periodic fraction. The non-periodical part of n digits, where $n=max(\alpha,\beta)$; the period contains at most (b_1-1) digits. (The period contains λ digits, where λ is the least divisor of $\lambda_M=Q(b)$ for which $10^2\equiv 1(mod\, b)$).

The transformation of the periodical decimal fractions in ordinary fractions

The generator fraction of a periodical simple decimal fraction (sub-unitary) has as denominator the number formed of the period and as numerator the number $10^n-1=99\underset{n}{...}9$, where 9 is the number of digits of the period.

$$0.(351)=\frac{351}{999}$$

The generator fraction of a periodic mixt decimal fraction (sub-unitary) has as numerator the difference between the number formed of the number formed by the non-periodic part followed by the periodic part and the number formed by the non-periodic part. As denominator we'll have the number written with digits 9 that are as many as the number of digits in the periodic part, followed by as many zeroes as the number of digits in the non-periodical part.

$$0.31(456)=\frac{31456-31}{99900}$$

Resolved problems

1) The period of fraction $\frac{a}{7},(7,10)=1,(a,7)=1$ is determined from the period of fraction $\frac{1}{7}$ moving a group of digits from the beginning to the end.

Example:

$$\frac{1}{7}=0,(142\ 857)$$

$$\frac{2}{7}=0,(285714)$$

$$\frac{3}{7}=0,(428571)$$

2) Prove that if in the sequence of the reminders of the division of the numbers $a,a\cdot 10,a\cdot 10^2,...,$ by the number b, where $(a,b)=1$ and $(b,10)=1$, there is the reminder $r_h=b-r_a$, then $r_{h+1}=b-r_1; r_{h+2}=b-r_2; ...; r_{h+n}=r_n$.

Deduct from here that the fraction's $\frac{a}{b}$ period has an even number of digits equal to $2h$, and that $\alpha+\beta=10^h-1$, where α is the number formed by the first h digits of the period, and β is the number formed by the last h digits of the period.

Example

$a=17;\ b=13$; the remainders are $r_a,r_1,r_2,...,r_i,....$

We have $a=b\cdot c+r_a$,

$$10r_a=b\cdot c_1+r_1$$
$$10r_1=b\cdot c_2+r_2$$
$$.....$$
$$10r_i=b\cdot c_{i+1}+r_{i+1}$$
$$.....$$

c_i are the period's digits.

But $r_h=b-r_a\Rightarrow 10r_h=10b-10r_a=10b-b\cdot c_1-r_1=b(9-c_1)+b-r_1;$

$r_{h+1}=b-r_1\Rightarrow 10r_{h+1}=10b-10r_a=10b-b\cdot c_2-r_2=b(9-c_2)+b-r_2;$

Therefore

$r_{h+1}=b-r_2$, etc.

We have

$$c_1+c_{n+1}=9$$
$$c_2+c_{n+2}=9 \quad \text{etc.}$$
$$\alpha+\beta=\underbrace{99...9}_{h\ times}=10^h-1$$

Example

$\frac{17}{13}$, its successive remainders are

$5;\ 11;\ 6;\ 8(=13-5);\ 2(=13-11);\ 7(=13-6)$

The period is $384\ 615$, and $384+615=999$.

3) Prove that the sum of the periods of the decimal fractions in which $\frac{a}{b},\frac{b-a}{b};(a<b;(b,10)=1;(a,b)=1)$ are transformed, is a number formed only from the digit 9.

$$\frac{a}{b}=\frac{P}{99...9}$$

$$\frac{b-a}{b}=\frac{P'}{99...9}$$

$$\frac{a}{b}+\frac{b-a}{b}=1+\frac{P+P'}{99...9}\Rightarrow P+P'=99...9$$

4) What ordinary fractions transform in decimal fractions with a one digit in the non-periodical part and two digits in the periodical part?

$$\frac{a}{b}=\overline{0,n(c_1c_2)}=\frac{\overline{n(c_1c_2)}-n}{990}$$

At the denominator it can be any divisor of 990, except those for 90 and 99:

$$\left.\begin{aligned}990&=2\cdot3^2\cdot5-11\\90&=2\cdot3^2\cdot5\\99&=3^2-11\end{aligned}\right\}$$ the numerator 22.55 or 110, etc. $(a,b)=1$

5) Prove that in the case of fraction $\frac{a}{b}$, through the division of a,b we obtain only prime numbers with b (smaller than b) as partial remainders $10^i a=b\cdot c+r_i$, if r_i and b would have a common divisor, then this divisor would divide also $10^i\cdot a$, which is impossible (because of the hypothesis).

Through the division of $\frac{a}{b}$, where $(a,)=1$, $(b,10)=1$, the period has at most $\varphi(b)$ digits; if the period has k digits, then $k/\varphi(b)$; where $\varphi(b)$ is the number of all prime numbers with b and inferior to it.

$$\varphi(b)=b\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_n}\right), \text{ or}$$

$$\varphi(b)=\left(p_1^{\alpha_1}-p_1^{\alpha_1-1}\right)\left(p_2^{\alpha_2}-p_2^{\alpha_2-1}\right)...\left(p_n^{\alpha_n}-p_n^{\alpha_n-1}\right), \text{ where } b=p_1^{\alpha_1}p_2^{\alpha_2}...p_n^{\alpha_n}.$$

Fractional units or principal fractions

Principal fractions are those fractions which have the numerator 1.

Example: $\frac{1}{13},\frac{1}{18},\frac{1}{2}$.

A set is called numerable if its elements can be arranged in a sequence $a_1,a_2,...,a_n$, that is, if it can be established a bi-univocal correspondence between the given set and the set of the natural numbers.

Between the set of rational numbers and the set of the points on an axis does not exist a bi-univocal correspondence (due to the fact that on the axis there are also the irrational numbers). Therefore the set of irrational numbers is not numerable.

Between the set of real numbers and the points on the axis there is a bi-univocal correspondence.

The union of two numerable sets is a numerable set.

Approximate calculations

Absolute error

The absolute error is the difference between the exact value of a number and its approximate value.

The error can go two ways: on the left side of the zero, and to the right side of the zero on the number's line.

When segments are measured, there we see errors.

Example: $AB = 6.35m \Rightarrow 6.35 < AB < 6.36$

To round a number (integer or decimal) of a certain order, the digits of lower order are substituted by zeroes (or we neglect them, if these are decimals), we leave the digit of that order unchanged if after it follows a smaller digit smaller than 5 or we increase it with one more unit.

Example 432.516 rounded to the hundredths will be 432.52.

Approximate values resulted from computations

1) When working with exact values, but the computation leads to an approximate value.
2) When working with approximate values, and the computations lead to an approximate result.

Solved problems

1) Between what limits is the aria of a rectangle knowing that $L = 10 - 11m$ and $l = 5 - 6m$?

$10 < L < 11$

$5 < l < 6$

$50 < L \cdot l < 66$

2) Between what limits is the difference of two segments $AB = 4 - 5cm$ and $CD = 1 - 3cm$?

$4 < AB < 5$

$1 < CD < 3$

$4 - 3 = 1 < AB - CD < 4 = 5 - 1$

Operations with approximated numbers

Addition

1) When we don't know the direction of the error

$a-\alpha<A<a+\alpha$

$b-\beta<B<b+\beta$

$c-\gamma<C<c+\gamma$

$$(a+b+c)-(\alpha+\beta+\gamma)<A+B+C<(a+b+c)+(\alpha+\beta+\gamma)$$

A,B,C are the exact values

a,b,c are the approximate values

α,β,γ are the approximations (the limits of errors)

The error limit of the sum is equal with the sum of the errors of the terms.

2) When we know the direction of the error

$a<A<a+\alpha$

$b<B<b+\beta$

$c<C<c+\gamma$

$$a+b+c<A+B+C<(a+b+c)+(\alpha+\beta+\gamma)$$

a,b,c are the values approximated in minus.

The sum of the approximate values in minus of the terms represents an approximate value in minus also, the limit of the error being equal to the errors' sum.

3) When we know the terms' errors

$A=a+l_1$

$B=b+l_2$

$C=c-l_3$

$A+B+C=(a+b+c)+l_1+l_2-l_3$

a,b,c are the values approximated in minus

l_1,l_2,l_3 are the errors

The exact value of a sum is equal to the sum of the approximate values of the terms plus the algebraic sum of the errors.

The most probable value of a measurement is the arithmetic average of the resultants found through several measurements, after the visible error have been eliminates.

Subtraction

If the direction of the error is unknown in the case of the difference's terms, then we'll not know the sense's error of the result, but is sure that the result's error is smaller than the sum of the terms' errors.

Multiplication

1) When we know the sense of errors

$$a-\alpha<A<a+\alpha$$
$$b-\beta<B<b+\beta$$
$$ab-(a\beta+b\alpha)+\alpha\beta<AB<ab+(a\beta+b\alpha)+\alpha\beta$$

$\alpha\beta$ is neglected being very small, then

$$ab-(a\beta+b\alpha)<AB<ab+(a\beta+b\alpha)$$
$$E(ab)=a\cdot E(b)+b\cdot E(a)$$

where

$E(a)=\alpha$, the error of A

$E(b)=\beta$, the error of B

2) When a and b represent approximate values in minus

$$a<A<a+\alpha$$
$$b<B<b+\beta$$
$$ab<AB<ab+(a\beta+b\alpha)+\alpha\beta$$
$$E(ab)=a\cdot E(b)+b\cdot E(a)$$
$$E(abc)=ab\cdot E(c)+ac\cdot E(b)+bc\cdot E(a)$$

Division

If the numerator is less that its exact value, and the denominator is greater than its exact value, the quotient will be smaller than the exact value, and if the numerator is larger than the exact value and the denominator is less than its exact value, the we'll obtain the quotient will be larger than the exact value.

$$12<a<16$$
$$2<b<3$$
$$\frac{12}{3}=4<\frac{a}{b}<\frac{16}{2}=8$$

The quotient's error

$$a-\alpha<A<a+\alpha$$
$$b-\beta<B<b+\beta$$
$$\frac{a-\alpha}{b+\beta}<\frac{A}{B}<\frac{a+\alpha}{b-\beta}$$
$$E\left(\frac{a}{b}\right)=\frac{aE(b)+bE(a)}{b\left[b-E(b)\right]} \qquad (3)$$

If a and b are approximate vales of the A and B with the approximate $E(a), E(b)$, for which we don't know the error's direction, then the $\frac{a}{b}$ is an approximate value of the exact quotient $\frac{A}{B}$, without knowing the error's direction, and the error limit is given by the relation (3)

The quotient's error when we know the approximate values in negative direction of the terms.

$$\begin{array}{l} a < A < a + \alpha \\ b < B < b + \beta \\ \hline \dfrac{a}{b+\beta} < \dfrac{A}{B} < \dfrac{a+\alpha}{b} \end{array}$$

Relative errors

The relative error is the quotient between the absolute error and the exact value of a number:

$$l = \frac{A - a}{A}$$

Example:

Let $A = 0.325$ and let $a = 0.3$ its tenth rounded value.

The absolute value is $A - a = 0.025$; the relative error is $\frac{0.025}{0.325} = \frac{1}{13}$.

If a number has m exact significant digits, the relative error is smaller than $\frac{1}{k \cdot 10^{m-1}}$ or smaller than $\frac{1}{10^{m-1}}$.

If is given that the relative error is smaller than $\frac{1}{(k+1) \cdot 10^{m-1}}$, where k is the first digit of the number, we deduct that the number has m exact digits.

If given $l < \frac{1}{10^m}$, because $\frac{1}{10^m} < \frac{1}{(k+1) \cdot 10^{m-1}}$, we deduct that m digits are exact.

The relative error of a product

$$l(a \cdot b) = l(a) + l(b)$$

$$l(abc) = l(a) + l(b) + l(c)$$

The relative error of a product is equal with the sum of the relative errors of the factors of the product.

The relative error of a ratio

$$l\left(\frac{a}{b}\right) \approx l(a) + l(b)$$

The relative error of a ratio is approximate equal to the sum of the relative errors of the terms.

Ratio and proportions

The irrational numbers are incommensurables; these cannot be measured exactly; in the decimal writing these have an infinite number of decimals, which are not is a periodic succession. Example is π

The fundamental property of a ratio

The ratio of two values is equal to the ratio of their measures in which it has been used the same measurement unit and it does not depend of the measurement unit used.

Proportions

The equality of two ratios is called proportion

$\frac{a}{b}=\frac{c}{d}$

a,d are the outer terms and are called extremes

b,c are the middle terms and are called means

The fundamental property of a proportion

The product of the extremes is equal to the product of the means.

Derived proportions

$\frac{a}{b}=\frac{c}{d}$

I) Derived proportions with the same terms

1) Interchange the means between them $\frac{a}{c}=\frac{b}{d}$
2) Interchange the extremes between them $\frac{d}{b}=\frac{c}{a}$
3) Invers the ratios $\frac{b}{a}=\frac{d}{c}$
4) Swap the ratios' places $\frac{c}{d}=\frac{a}{b}$
5) Simultaneously swap the extremes and the means between them $\frac{d}{c}=\frac{b}{a}$

II) Derived proportions with the terms swapped

1) Multiply the numerators with the same number
2) Divide the numerators by the same number
3) Multiply the denominators with the same number
4) Divide the denominators by the same number
5) Amplify the both ratios or only one ratio by the same number
6) Simplify the ratios or only ratio with the same number

7) Multiply the two ratios by another ratio $\frac{a}{b}=\frac{c}{d}\Rightarrow\frac{am}{bn}=\frac{cm}{dn}$

8) The ratio of the sum of the numerators and the sum of the denominators is equal to each of the given ratios $\frac{a}{b}=\frac{c}{d}=\frac{a+c}{b+d}$

9) The ratio of the difference of the numerators and the difference of the denominators is equal to each of the given ratios $\frac{a+c}{b+d}=\frac{a-c}{b-d}$

10) The ratio of the sum of the numerators and the sum of denominators is equal to the ratio of the difference of the numerators and he difference of the denominators $\frac{a+c}{b+d}=\frac{a-c}{b-d}$

III) Derived proportions by changing in the same mode each ratio, through linear combinations between terms

1) The ratio formed by adding the numerator with the denominator $\frac{a+b}{b}=\frac{c+d}{d}$ and denominators unchanged

2) The ratio formed by subtracting from the numerator the denominator, and leave the denominators unchanged $\frac{a-b}{b}=\frac{c-d}{d}$

3) The ratio formed by adding the numerator with the denominator and replace the denominator by the numerator $\frac{a+b}{a}=\frac{c+d}{c}$

4) The ratio formed by subtracting from the numerator the denominator, and replace the denominator by the numerator $\frac{a-b}{a}=\frac{c-d}{c}$

5) The ratio formed by the unchanged numerators and as denominators we add to the denominator the numerator $\frac{a}{b+a}=\frac{c}{d+c}$

6) The ratio formed by the unchanged numerators and as denominators we subtract from the denominator the numerator $\frac{a}{b-a}=\frac{c}{d-c}$

7) The ratio formed by replacing the numerators with the denominators and as denominators we have the sum of the numerator and denominator $\frac{b}{b+a}=\frac{d}{d+c}$

8) The ratio formed by replacing the numerators with the denominators and as denominators we have the difference between the numerator and denominator $\frac{b}{b-a}=\frac{d}{d-c}$

$$\frac{a}{b}=\frac{a'}{b'}\Rightarrow\frac{ma+nb}{pa+qb}=\frac{ma'+nb'}{pa'+qb'}$$

$$\frac{a}{b}=\frac{a'}{b'}\Rightarrow\frac{m_1a^2+m_2ab+m_3b^2}{n_1a^2+n_2ab+n_3b^2}=\frac{m_1a'^2+m_2a'b'+m_3b'^2}{n_1a'^2+n_2a'b'+n_3b'^2}$$

Average proportions

The average of two given numbers a and b is the number m determined such that the ratios $\frac{a}{m}$ and $\frac{m}{b}$ have the same value $\frac{a}{m}=\frac{m}{b}\Rightarrow m^2=ab\Rightarrow ab\Rightarrow m=\sqrt{ab}$

The averages of the form $\frac{a}{a}=\frac{a'}{a'}$ or $\frac{a}{b}=\frac{a}{b}$ are not considered true proportions.

Multiple equal proportions

$$\frac{a_1}{b_1}=\frac{a_2}{b_2}=\frac{a_3}{b_3}=\frac{a_1+a_2+a_3}{b_1+b_2+b_3}$$

If two or more ratios are equal, the ratio of the sum of the numerators and the sum of the denominators is equal to the given ratios.

The division of a number in proportional parts with given numbers

Example: Divide 176 in proportional parts with the numbers 7; 10; 15.

$$\frac{x}{7}=\frac{y}{10}=\frac{z}{15}=\frac{x+y+z}{7+10+15}=\frac{176}{32}$$

$$\frac{x}{7}=\frac{176}{32}\Rightarrow x=38\frac{1}{2}$$

$$\frac{y}{10}=\frac{176}{32}\Rightarrow y=55$$

$$\frac{z}{15}=\frac{176}{32}\Rightarrow z=82\frac{1}{2}$$

The division of a number in invers proportional parts with given numbers

Example: Divide 315 in invers proportional parts with the numbers 6; 10; 12

$$\frac{x}{\frac{1}{6}}=\frac{y}{\frac{1}{10}}=\frac{z}{\frac{1}{12}}=\frac{x+y+z}{\frac{1}{6}+\frac{1}{10}+\frac{1}{12}}=\frac{315}{\frac{21}{60}}$$

$$\frac{x}{\frac{1}{6}}=\frac{315}{\frac{21}{60}}\Rightarrow x=15$$

$$\frac{y}{\frac{1}{10}}=\frac{315}{\frac{21}{60}}\Rightarrow y=9$$

$$\frac{z}{\frac{1}{12}}=\frac{315}{\frac{21}{60}}\Rightarrow z=7.5$$

Direct proportional measures

Direct proportional measures are those measures that depend one of the other such that if one increases n times ($n \in N$) the other increases by the same number of times, (the same when we decrease).

Theorem

The ratio of two values of one of the measures is equal to the ratio between the corresponding values of the other measure.

Invers proportional measures

Invers proportional measures are those measures that depend one of the other such that if one increases n times ($n \in N$) the other decreases by the same number of times.

Theorem

The ratio of two values of one of the measures is equal to the invers of the ratio between the corresponding values of the other measure.

The fundamental rule of proportions

Example: In a cylindrical recipient there is stored gas under pressure; its volume is $8cm^3$ and the pressure is 5atm. If the containers' piston is raised such that the gas volume becomes $20cm^3$, what will be its pressure?

$$\begin{array}{l} 8cm^3 \overset{i}{\ldots} 4atm \\ 20cm^3 \ldots x\ atm \\ \hline x = \dfrac{8 \cdot 5}{20} = 2atm \end{array}$$

(The V and P are invers proportional by the law of Boyle-Mariotte).

In general, the measures can be dependent or independent.

The compound proportions' fundamental rule

At a farm, the quantity of $1400Kg$ stored grasses is needed to feed 10 cows for 7 days. In how many days 2 cows will consume $8000Kg$ of grasses?

1)

$$\begin{array}{l} 1400Kg \overset{d}{\ldots} 10cows \overset{i}{\ldots} 7days \\ 8000Kg \ldots 2cows \ldots x days \\ \hline \dfrac{x}{7} = \dfrac{10}{2} \cdot \dfrac{8000}{1400} \Rightarrow x = 200days \end{array}$$

2)

$$\begin{array}{l} 1400Kg \overset{d}{\ldots} 10cows \overset{i}{\ldots} 7days \\ 8000Kg \ldots 2cows \ldots x days \\ \hline x = \dfrac{10 \cdot 7 \cdot 8000}{1400 \cdot 2} \Rightarrow x = 200days \end{array}$$

3)

$1400Kg \overset{d}{..} ....10cows \overset{i}{..} .....7days$

$8000Kg .....10cows .....x' days$

$$x' = \frac{8000 \cdot 7}{1400} days$$

$1400Kg \overset{d}{..} ....10cows \overset{i}{..} ..... \frac{8000 \cdot 7}{1400} days$

$8000Kg .....2cows .....x days$

$$x = \frac{10 \frac{8000 \cdot 7}{1400}}{2} \Rightarrow x = 200 days$$

4) **The method of reduction to the unit**

$1400Kg \overset{d}{..} ....10cows \overset{i}{..} .....7days$

$1400Kg \overset{d}{..} ....1cow .....7 \cdot 10 days$

$1Kg .....1cow ..... \frac{7 \cdot 10}{1400} days$

$8000Kg .....1cow ..... \frac{7 \cdot 10}{1400} \cdot 8000 days$

$8000Kg .....2cows ..... \frac{7 \cdot 10 \cdot 8000}{1400 \cdot 2} days = 200 days$

Percentages

$$p\% = \frac{p}{100}$$

$$p \text{ } ‰ = \frac{p}{1000}$$

Ratio to percentage

A percentage is another way of describing a ratio with respect to 100

a) Finding the percentage from a number:

$$p\% \text{ from } A = A \cdot \frac{p}{100}$$

b) Finding the ratio percentage of a number in relation to another number A

$A .....a$

$100 .....x$

$$x = 100 \cdot \frac{a}{A}$$

Successive percentages

If

$$\frac{a}{b}=\frac{c}{d}\Rightarrow\frac{ka+hb}{k'a+h'b}=\frac{kc+hd}{k'c+h'd},\ \left(\forall k,h,k',h'\notin N\right)$$

and

$$\frac{ka^2+hab+lb^2}{k'a^2+h'ab+l'b^2}=\frac{kc^2+hcd+ld^2}{k'c^2+h'cd+l'd^2}$$

Periodical simple fractions

If $\left(a,b\right)=1$ and $\left(b,10\right)=1\Rightarrow\frac{a}{b}$ is a periodical simple fraction.

The maximum number of digits of a period is $\lambda_M=\varphi\left(b\right)$, where $\varphi\left(b\right)$ is Euler's function

The exact number of digits of a period is λ, which is the smaller among the divisors λ_M, which, as exponent of the base 10, gives the remainder by the division to the numerator b; therefore λ/λ_M, $\left(10^2\equiv1\left(mod\,b\right)\right)$.

Example: Find the number of digits of the period of $\frac{1}{7}$, and then write directly the remaining divisions: $\frac{2}{7},...,\frac{6}{7}$.

$\left(1,7\right)=1$ and $\left(7,10\right)=1\Rightarrow\frac{1}{7}$ the periodical fraction simple

$\lambda_M=\varphi\left(7\right)=6\Rightarrow\lambda=1,2,3$ or 6

$$\left.\begin{aligned}10^1&\equiv3\left(mod\,7\right)\\10^2&\equiv2\left(mod\,7\right)\\10^3&\equiv6\left(mod\,7\right)\\10^6&\equiv1\left(mod\,7\right)\end{aligned}\right\}\Rightarrow\lambda=6=\text{the number of digits of the period.}$$

$$\frac{1}{7}=0.\left(142857\right)$$

Table:

r	1	3	2	6	4	5	partial remainders
c	1	4	2	8	5	7	corresponding ratios

$\Rightarrow\frac{2}{7}=0.\left(264513\right)$, $\frac{5}{7}=0.\left(714285\right)$

There are the same digits in the period, but in other positions.

The number of tables necessary to write all divisions of the form $\frac{x}{b}$, where $\left(x,b\right)=1\left(\left(b,10\right)=1\right)$ is equal to $\frac{\lambda_M}{\lambda}$; in the case when we have multiple tables, it will be

considered another division $\frac{y}{x}$ such that the remainder $y < x$ not to be among the remainders of the first table (or on other tables). In our case $\frac{6}{6} = 1$ (only one table)

The division of a number in direct proportional parts by a number and invers proportional with another number (simultaneously)

The construction of a road between two small towns was valued to $190,000. Find the contribution of each town knowing that the amount was proportional with the population of each town and invers proportional to the distance of each village to the road. First town has 5000 residents and the distance to the road is 3Km. Second town has 3000 residents and the distance to the road is 2Km

$$\frac{x}{5000 \cdot \frac{1}{3}} = \frac{y}{3000 \cdot \frac{1}{2}}$$

$$\frac{x}{\frac{10000}{6}} = \frac{y}{\frac{9000}{6}}$$

$$\frac{x}{10000} = \frac{y}{9000} = \frac{190000}{19000} = 10 \Rightarrow x = 100000; y = 90000$$

Show that the product of three consecutive numbers cannot be the perfect cube of a natural number.

$n^3 < n^3 + 3n^2 + 2n < n^3 + 3n^2 + 3n + 1$.

Chapter T□ o: Plane Geo□ etry

Fundamental notions of the elementary geometry (Euclidean):

a) The point
b) The line
c) The plane

The axioms are truths which need to be proved.

The postulates are evident truths, which are not proved.

Theorem

Lemmas are helping statements that will help understand a theorem.

Corollary is an immediate consequence of a theorem.

Proposition is a statement.

The theorems can be

a) Direct $I \Rightarrow C$
b) Converse $C \Rightarrow I$
c) Contrary $nonI \Rightarrow nonC$
d) Contrary converse $nonC \Rightarrow nonI$

The method of reduction ad absurdum consists in the process of supposing the contrary, and based on the law of the excluded third (a proposition cannot be other than false or true).

Example:

Direct theorem: the diagonals of a rhombus are perpendicular (true)

The converse theorem: If the diagonals of a quadrilateral are perpendicular, then the quadrilateral is rhombus (false)

Contrary theorem: If a quadrilateral is not a rhombus, its diagonals are not perpendicular (false)

Contrary converse theorem: If the diagonals of a quadrilateral are not perpendicular, then the quadrilateral is not a rhombus (true).

Lines

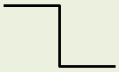
1) Line segment
2) Semi line
3) Line

Lines:

a) Polygonal line

- Closed – polygons

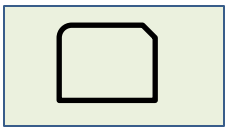
- Open



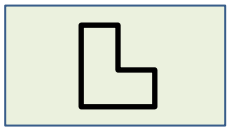
b) Curves (circle, ellipse, etc.)

Polygons

1. Convex – when the extension of any of its sides does not intersect any other of its sides

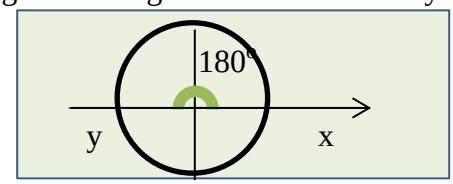


2. Concave – when the extension of at least one of its sides intersects another side of the polygon.

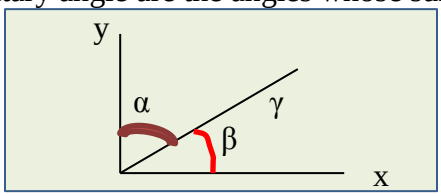


Angles

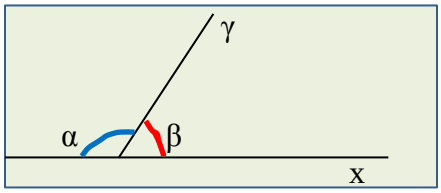
a) Straight angle is an angle that is 180° exactly



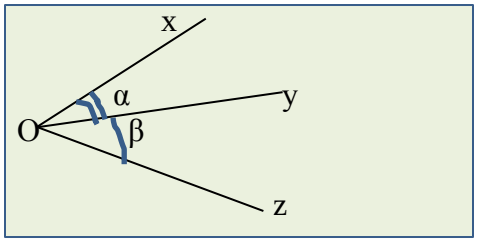
b) Complementary angle are the angles whose sum is 90^0



c) Supplementary angles are the angles whose sum is equal to 180^0



d) Adjacent angles are the angles which have a common side, same vertex and the other sides are on different part of the common side.



Theorem

On a point of a line it can be constructed only one perpendicular line.

From an external point of a line only one perpendicular line can be constructed on a given line.

All right angles are equal.

All straight angle are equal

The circle is the set of point from a plane whose distances to fixed point are equal.

The angle at the center is the angle whose vertex is in the center of the circle.

Theorem

In one circle or several equal circles to equal angles at the center correspond equal arcs, and to unequal angles at the center correspond unequal arcs; to the larger angle at the center corresponds the larger arc.

The measure of the angle at the center is equal to the measure of arc between its sides.

The sum of the angles formed around one point is 360^o.

Theorem

The angles whose vertexes are opposite are (called also vertically opposite angles) equal.

Converse

If a line forms equal angles with two semi lines, which have the same origin on that line, and are placed on the sides of line, and are not adjacent, then the semi lines are straight.

Triangles

A triangle is the polygon with three sides.

1) Triangles can be classified by the relative lengths of their sides:
   a) Equilateral ($L_1 = L_2 = L_3$)
   b) Isosceles $L_1 = L_2$
   c) Scalene (all sides are different)

2) Triangles can be classified by the internal angles:
   a) Right-angled triangle (rectangle triangle)
   b) Obtuse-angled triangle(obtuse triangle)
   c) Acute angled triangle (oblique triangles)

The exterior angle of a triangle is the angle formed by a side and the extension of another side; it is equal to the sum of the other two interior angles of the triangle.

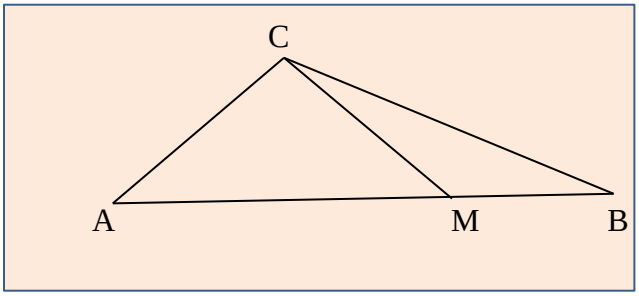
Important lines in a triangle

1) The height or the altitude in a triangle is the perpendicular segment from a vertex to its opposite side. The altitudes are concurrent and their intersection point is called **orthocenter**.
2) The median in a triangle is a line segment from a vertex of the triangle to the midpoint of the side opposite that vertex. There are three medians and all are

concurrent in point called **centroid**. The centroid is on the median at $\frac{2}{3}$ from the vertex and $\frac{1}{3}$ from the base.

3) The bisector in a triangle is the line segment that equally divides the angle of the triangle. There are three bisectors, which are concurrent in a point called the center of the inscribed circle in that triangle.
4) The perpendicular bisector in a triangle is the perpendicular line on the middle side of the triangle. There are three perpendicular bisectors in a triangle and they are concurrent in a point which is the center of the circumscribed circle to the triangle.

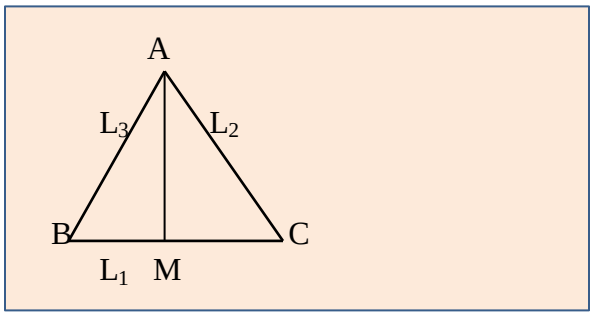
A cevian is any line segment in a triangle with one endpoint on a vertex of the triangle and the other endpoint on the opposite side.



CM = cevian from the mathematician Giovanni Ceva.

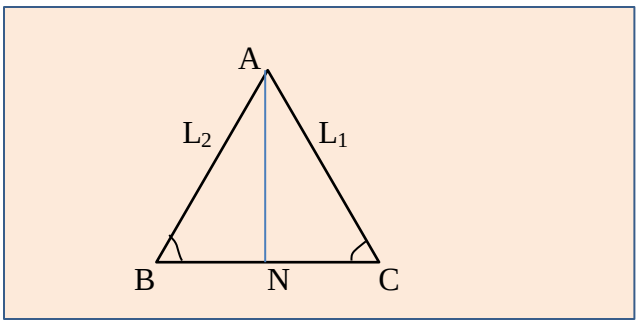
The properties of an equilateral triangle

a) $L_1 = L_2 = L_3$
b) $\sphericalangle A = \sphericalangle B = \sphericalangle C = 60^o$
c) The altitudes are also medians, bisectors, and .perpendicular bisector.



The properties of the isosceles triangle

a) $L_1 = L_2$
b) The angles opposite to the equal sides are equal.
c) The altitude corresponding to the base of the triangle is median and perpendicular bisector



The cases of equality of two random triangles

First Case (A.S.A) a side and two joint angles respectively equal
Second Case (S. A. S) two sides and the angle between them respectively equal
Third Case (S.S.S) all sides respectively equal

The cases of equality of two rectangle triangles

a) A cathetus and an acute angle respectively equal
b) Hypotenuse and an acute angle respectively equal
c) The two catheti are respectively equal
d) The hypotenuse and a cathetus are respectively equal
e)

An exterior angle of a triangle is greater than any interior angle not joint to it.

Relations between the sides and the angles of a triangle

In a triangle the greater side is opposite to the greater angle.
Converse: the greater angle is opposite to a greater side.

Inequalities between the sides of a triangle

a) In a triangle a side is greater than the difference of the other two sides and smaller than their sum:

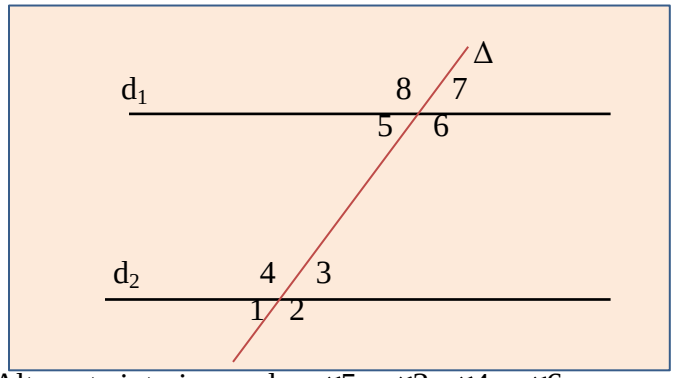
$a > b - c$ $\qquad$ $a < b + c$

$b > a - c$ $\qquad$ $b < a + c$

$c > a - b$ $\qquad$ $c < a + b$

If two triangles have each two equal sides and the angles between them not equal, then to the greater angle opposes the greater side.

Angles formed by two parallel lines intersected by a secant.



1) Alternate interior angles $\sphericalangle 5 = \sphericalangle 3;\ \sphericalangle 4 = \sphericalangle 6$
2) Alternate external angles $\sphericalangle 2 = \sphericalangle 8;\ \sphericalangle 1 = \sphericalangle 7$
3) Corresponding angles
$$\sphericalangle 1 = \sphericalangle 5;\ \sphericalangle 2 = \sphericalangle 6$$
$$\sphericalangle 4 = \sphericalangle 8;\ \sphericalangle 3 = \sphericalangle 7$$
4) Interior of the same side $\sphericalangle 4 + \sphericalangle 5 = 180^0$
5) External of the same side $\sphericalangle 1 + \sphericalangle 8 = 180^0$

If two lines intersected by a secant forms alternate interior equal angles or alternate external or corresponding equal angles then the two lines are parallel.

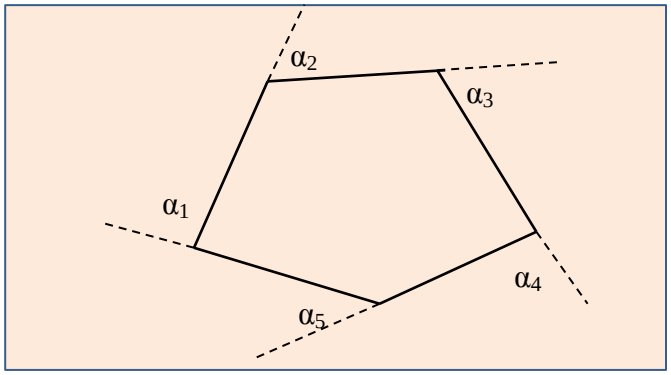
Two angles with the sides respectively parallel are equal only if both angles are acute or supplementary if one of them is obtuse and the second one is acute.

Two angles with the sides respectively perpendicular are equal if both are acute or obtuse, or supplementary if one is acute and the other is obtuse.

The sum of the angles of a triangle is $180^{0.}$

The sum of the interior angles of polygon convex with n sides is equal to $180^0(n-2)$.

The sum of the external angles of a convex polygon formed by the extensions of the sides in the same direction is equal to 360^0, (therefore, is independent of the number of the sides)



$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 = 360^0$$

Geometrical loci

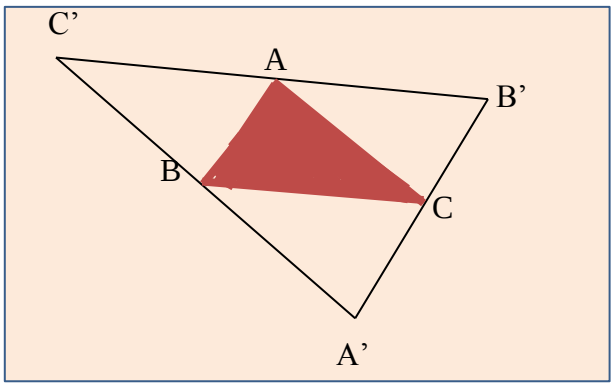
Any point on the perpendicular bisector is equally positioned from the segment's extremities and conversely: any point equally positioned from the extremities of a segment, will be on the perpendicular bisector of that segment.

A geometrical locus is a geometric figure formed by the set of points which have the same property.

Any point on the bisector of an angle is at equal distance from the sides of the angle, and conversely: any point at the equal distance from the sides of an angle it will be on the bisector of that angle.

The geometrical locus of the points at an equal distance of two concurrent lines is formed by two perpendicular lines, the bisectors of the angle formed by the lines.

The anticomplementary triangle to a given triangle ABC is the triangle which is formed by constructing parallels to the opposed sides through each vertex of the given triangle.



$\Delta A'B'C'$ is the anticomplementary triangle of ΔABC.

Two points C,D which divide the side AB in the same ratio are called harmonic conjugate (one interior and the other exterior)

Quadrilaterals

A quadrilateral is a polygon with four sides.

Parallelogram

A parallelogram is a quadrilateral whose sides are parallel two by two.

Properties

The opposite angles of a parallelogram are equal.
The adjacent angles of a parallelogram are supplementary.
The opposite sides of a parallelogram are equal two by two.
(The parallel lines contained between parallel lines are equal)

The diagonals of a parallelogram intersect forming on each diagonal equal segments.

The sufficient and necessary conditions for a quadrilateral to be a parallelogram:

a) The opposite sides to be parallel two b two
b) The opposite sides to be equal two by two
c) The opposite angles to be equal two by two
d) The diagonals to split in equal segments
e) Two sides (opposed to each other) to be equal between them and parallel

Rhombus

The rhombus is a parallelogram with two adjacent equal sides.

Properties

The diagonals of a rhombus are perpendicular
The altitudes of a rhombus are equal.

Rectangle

A rectangle is a parallelogram with a right angle.

Properties

The diagonals of a rectangle are equal

The median relative to the hypotenuse of a right angle triangle is equal to half of the hypotenuse.

In right triangle the cathetus which is opposite to the angle of 30^0 is equal to half of the hypotenuse.

Converse: If in a right angle triangle a cathetus is equal to half of the hypotenuse, then it opposes to an angle of $30^{0.}$

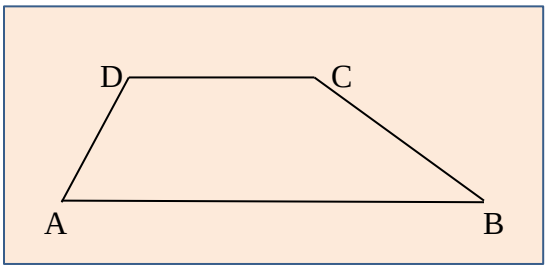
Square

A square is the rhombus with a right angle or a rectangle with two adjacent sides equal.

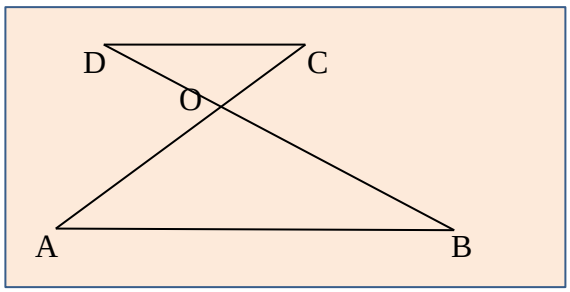
A polygon regular is a polygon which has all sides equal and all angles equal.

Trapezoid

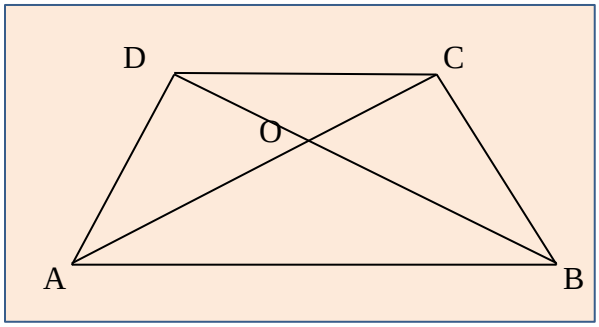
A trapezoid is a quadrilateral with at least two parallel sides.
A trapezoid can be convex



or concave

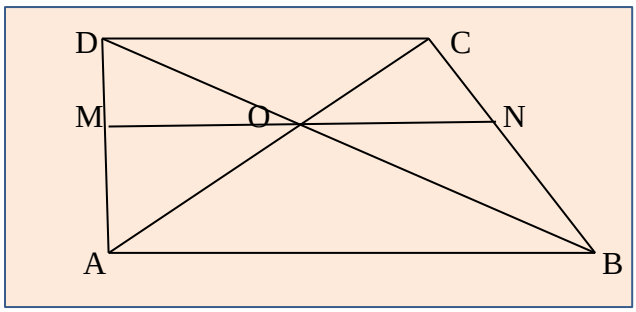


The isosceles trapezoid is the trapezoid in which the sides which are not parallel are equal.



$AO = OB; DO = OC$

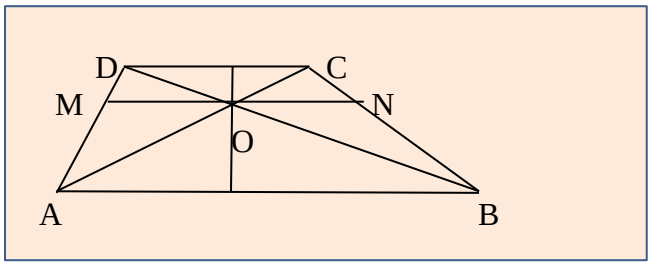
The **right angle trapezoid** is trapezoid which has a right angle (this implies that there is another right angle in that quadrilateral)



The angles adjacent to the bases of an isosceles trapezoid are equal, and the remaining two are supplementary, and converse.

The diagonals of an isosceles trapezoid make with each of the bases equal angles.

Relations in a random trapezoid



$$Aria = \frac{(B+b)\cdot I}{2}$$

If $MON \| AB$ then

1) $OM = ON$ 2) $\frac{CN}{NB} = \frac{DM}{MA} = \frac{DC}{AB}$

Geometrical loci

The geometric locus of the set of points at given distance from a line is formed by a parallel line to the given line and at the given distance.

The geometric locus of the set of points for which the ratio of the distances to two parallel lines is constant is formed of two parallel lines to the given lines.

The geometric locus of the set of points for which the ratio of the distances to two concurrent lines is constant and it is formed by two lines which are concurrent to the given lines.

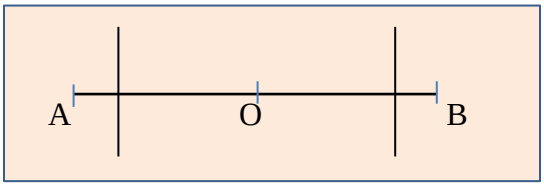
The geometric locus of the set of points from which a line segment can be seen under an angle of 90^0 is a circle which has as diameter the given segment.

The geometric locus from which a given segment can be viewed under a given angle is formed by two arcs of circle of the given angle and which has their extremities coincide to the ends of the segment and are symmetric with respect to the given segment.

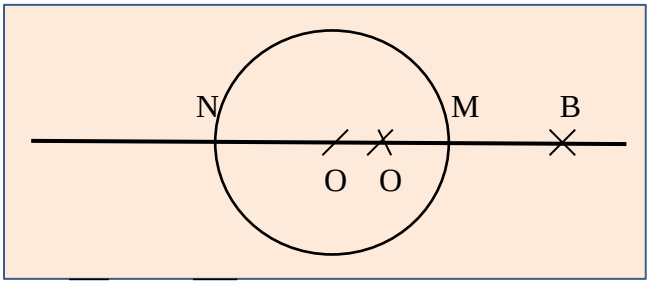
The geometric locus of the points for which the sum of the squared distances to two given fixed points is a constant is formed of a circle whose diameter is the line which connects the given points.

The geometric locus of the points which have equal powers with respect to two given circles is the radical axis of the two circles.

The geometric locus of the points for which the absolute value of the difference of their squared distances to two fixed points is constant, is formed from two perpendicular lines which connect the two points and are symmetric in relation to the segment's middle point which connects the two points.



The geometric locus of the points for which the ratio of the distances to two given points is equal to a given ratio k, is the circle whose diameter is the segment whose extremities are in the point which divides the given segment in the ratios $\pm k$ (the Greek mathematician Apollonius' circle).



$\frac{\overline{NA}}{\overline{NB}} = k$, $\frac{\overline{MA}}{MB} = -k$

Circle

The position of point with respect to a circle

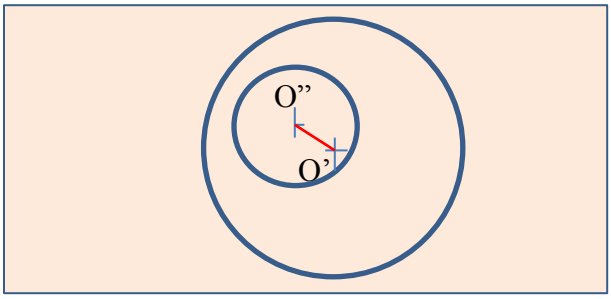
1) Interior to the circle
2) On the circle
3) Exterior to the circle

The position of line with respect to a circle

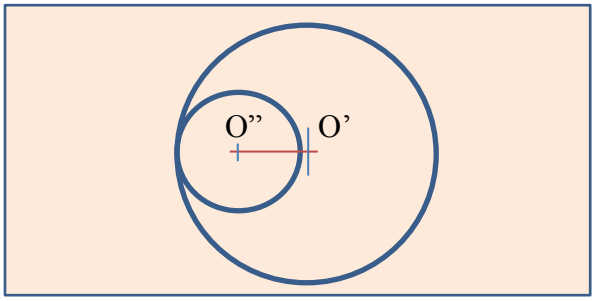
1) Secant (intersects the circle in two distinct points $d < R$
2) Tangent (has just one point in common with the circle $d = R$)
3) Exterior (it does not have any points in common with the circle $d > R$)

The position of two circles

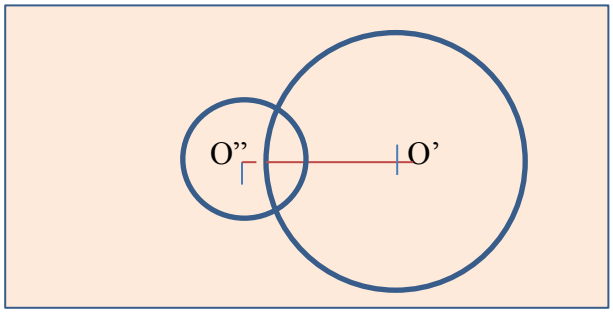
1) Interior circles $d > R_2 - R_1$



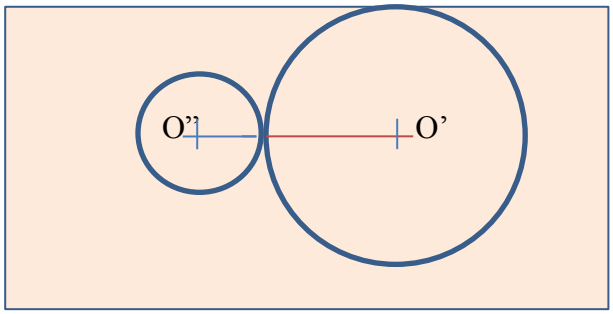
2) Tangent interior $d = R_2 - R_1$



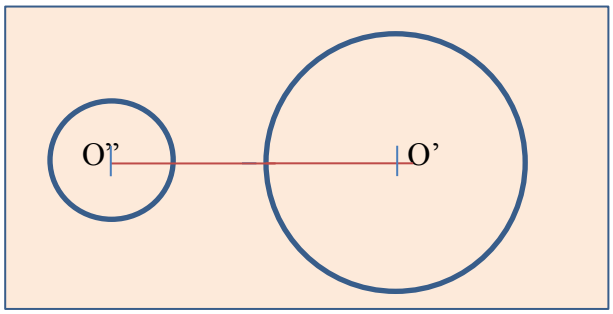
3) Secant $R_2 - R_1 < d < R_2 + R_1$



4) Tangent exterior $d = R_2 + R_1$



5) Exterior $d > R_2 + R_1$



The centers’ line is the line that connects the centers of two circles.
Through a point pass an infinity of circles

Through two points pass an infinity of circles

Through three non collinear points passes only one circle whose center is at an equal distance of the given points, and whose center is at the intersection of the perpendicular bisectors determined by these points.

The perpendicular diameter on a cord bisects it (bisects also the corresponding arc of the cord)

The normal to a circle in one of its points is the perpendicular constructed on the tangent at the circle in that point; therefore it is one of circle's radiuses.

In the same circle or in equal circles, the cords at the same distance to the center are equal.

In the same circle or in equal circles, the unequal cords are at an unequal distance from the center, the largest cord being closest to the center.

The diameter of a circle is the largest cord in the circle.

In the same circle or in equal circles, to any equal arcs correspond equal cords.

In the same circle or in unequal circles to unequal arcs (larger than the semicircle) correspond unequal cords and to the largest arc corresponds the largest cord.

The arcs contained between parallel cords are equal.

The common point of two circles is on the circle's line.

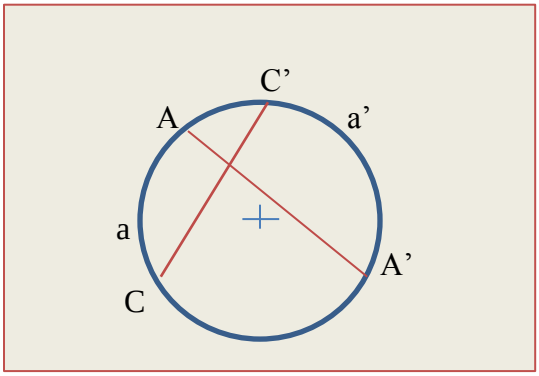
The tangents constructed from the same point to the circle are equal.

The line that connects the middle points of two parallel cords is the diameter perpendicular on the cords.

Angle inscribed in a circle is the angle whose vertex is on the circle and its sides are cords in the circle (or a cord and a tangent).

The measure of angle interior to a circle is equal to half of the sum of the measures of the arcs contained between the sides of the angle and their extensions.

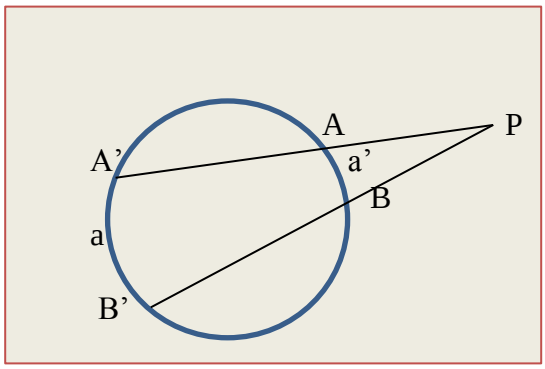
$$m\left(\sphericalangle ABC\right)=\frac{m\left(AaC\right)}{2}+\frac{m\left(A'a'C'\right)}{2}=\frac{m\left(AaC\right)+m\left(A'a'C'\right)}{2}$$



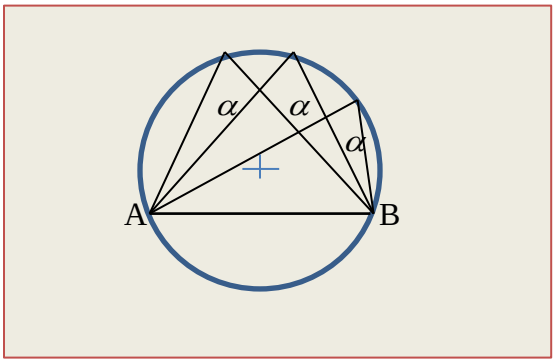
Angle exterior to a circle is the angle whose vertex is in the exterior of the circle, and its sides are secant or tangent to the circle.

The measure of an angle exterior to a circle is equal to half of the difference of the measures of the arcs contained between the sides of the angle.

$$m\left(\sphericalangle A' PB'\right) = \frac{m\left(A'a'B'\right) - m\left(AaB\right)}{2}$$



Arc subtended by a given angle



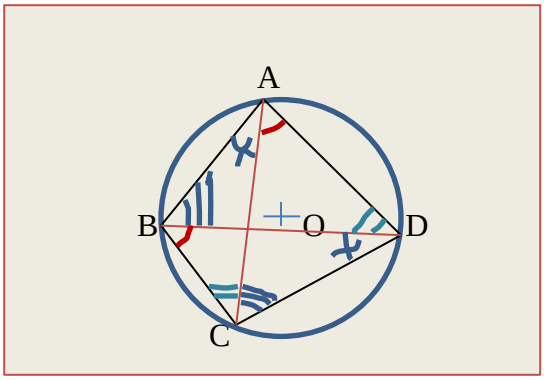
From the points of this arc, a segment can be viewed by the same angle α.

Inscribable quadrilaterals

The quadrilaterals which have all their vertexes on a circle are called inscribable quadrilaterals.

In a inscribable quadrilateral the angle formed by one of its diagonal with a side is equal to the angle formed by the other diagonal with the opposite side.

$ab = cd$



The opposed angles of an inscribable quadrilateral make together 180^0 (are supplementary).

First Theorem of Ptolemy

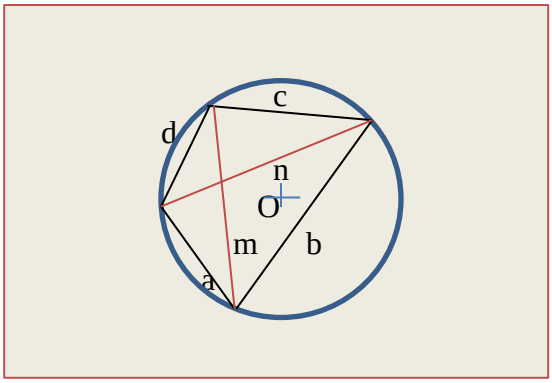
In an inscribable quadrilateral the sum between the products of the opposite sides is equal to the product of the diagonals:

$$a \cdot c + b \cdot d = m \cdot n$$

Second Theorem of Ptolemy

In an inscribable quadrilateral takes place the following relation:

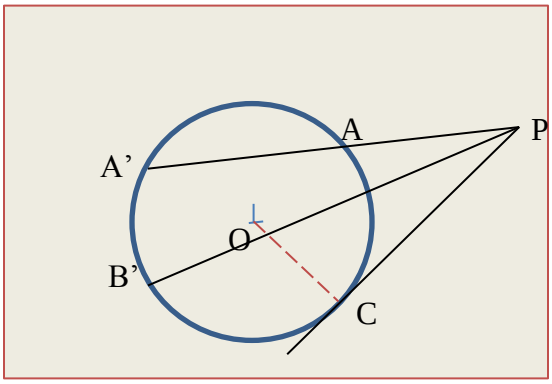
$$\frac{m}{n} = \frac{a \cdot b + c \cdot d}{a \cdot d + b \cdot c}$$



The power of a point in relation to circle

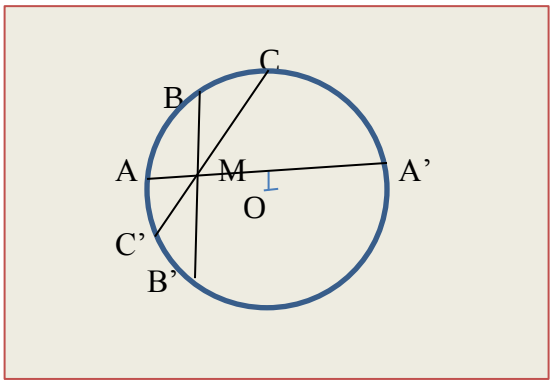
a) When the point is exterior to the circle:

$$PA \cdot PA' = PB \cdot PB' = ... + PC^2 = \text{constant}$$

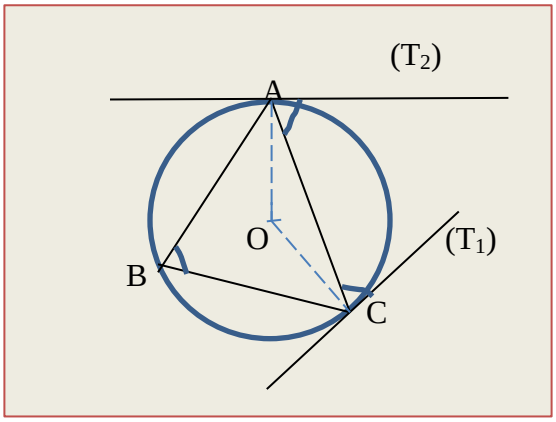


b) The point is interior to the circle

$$MA \cdot MA' = MB \cdot MB' = MC \cdot MC' = ... = \text{constant}$$

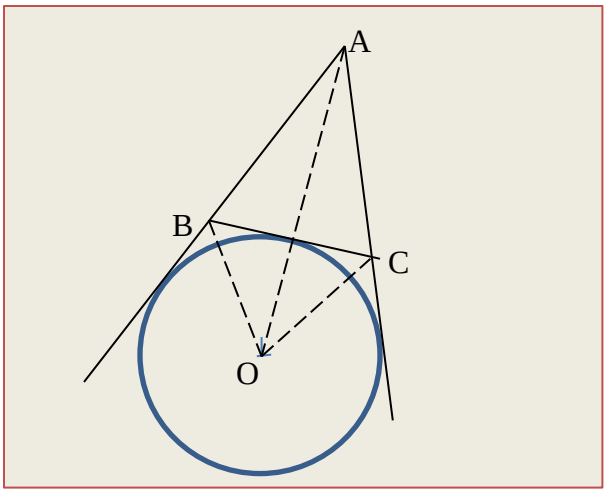


In an inscribed triangle in a circle, an angle is equal to the angle formed by the opposed side to the tangent in one of its ends.



Excircle or escribed circle to triangle

Excircle or escribed circle to triangle is the circle tangent to all sides of the triangle; to a triangle can be escribed three triangles.



$$\frac{1}{r_a}+\frac{1}{r_b}+\frac{1}{r_c}=\frac{1}{R}$$

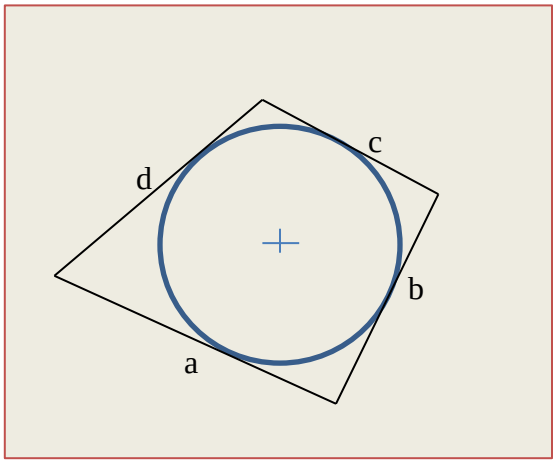
The center of this circle is at the intersection of the interior bisector with the external bisectors of the other angles.

The center of the circumscribed circle to a polygon is at the intersection of all perpendicular bisectors of the polygon. If these are not concurrent, then the polygon cannot be inscribed in a circle.

The center of the circumscribed circle to a right angle triangle is at the middle point on the hypotenuse.

The center of the inscribed circle in a polygon is at the intersection of the interior bisectors of all angles. If bisectors are not concurrent then the polygon is not circumscribable.

If a quadrilateral is circumscribed to a circle, the sum of two opposed sides is equal to the sum of the other two sides and converse.

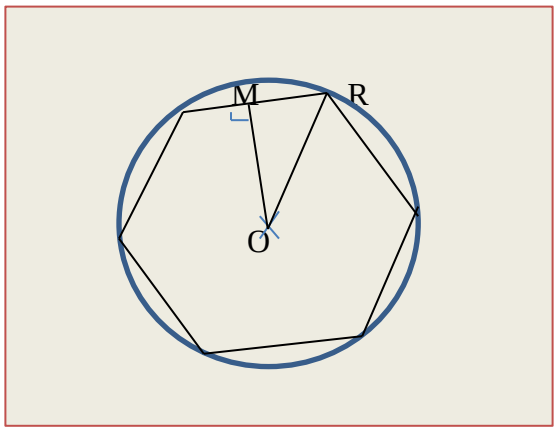


Regular polygons

Regular polygon is a polygon convex with all sides equal and all angles equal.

If a circle is divided in n equal arcs and then connect these consecutive points, we obtain a regular polygon with n sides.

For any regular polygon there is a circumscribable circle, and in any regular polygon we can inscribe a circle.

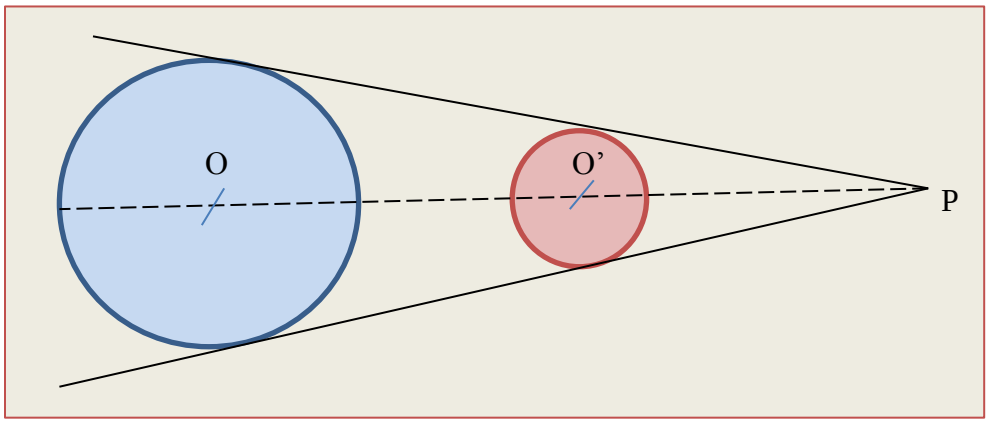


$$l_n = 2R\,sin\frac{180°}{n}$$

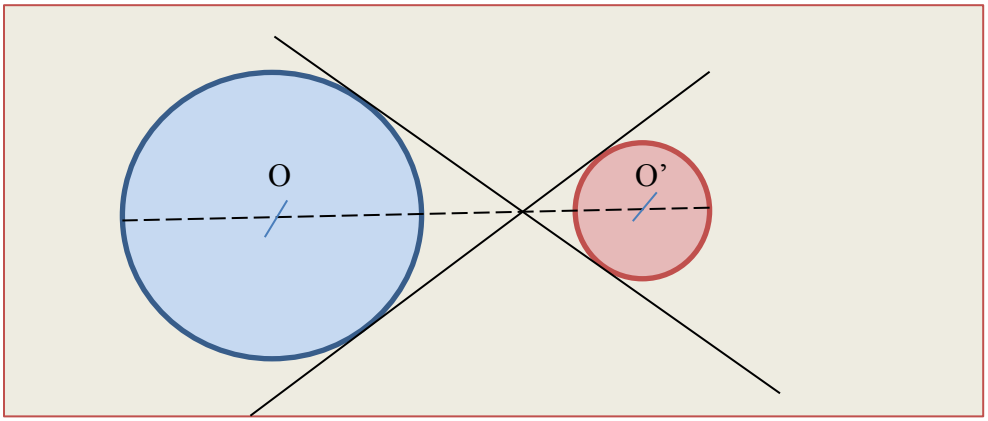
$$a_n = R\,cos\frac{180°}{n}$$

OR is the radius of the circumscribed circle
OM is the apothem of the regular polygon

The common tangent exterior of two circles



The common tangent interior of two circles



For the polygon with n sides ($n>3$) the sides' equality does not implies their angles' equality.

Dividing a circle in n equal arcs ($n>2$) and constructing tangents to the circle in these points, it is obtained a regular polygon circumscribed to the circle.

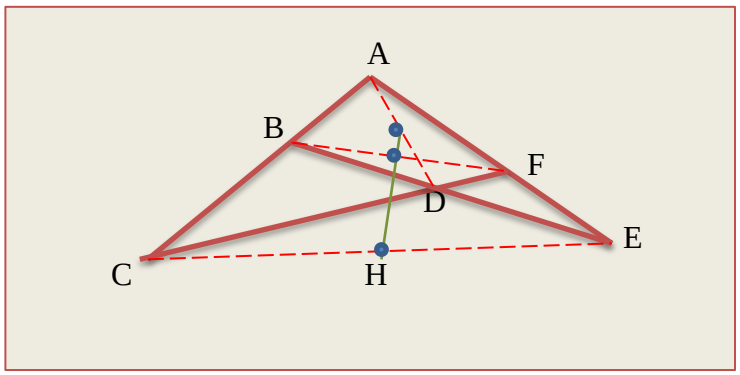
The centers of the inscribed and circumscribed circles to a regular polygon coincide.

The regular polygons can be:
a) Convex
b) Concave

Quadrilateral complete

A polygon formed by four coplanar lines (three of them should not be concurrent) is called a complete quadrilateral.

A complete quadrilateral has 4 sides, six vertexes and three diagonals



The middle points of the three diagonals are collinear.

Gauss' Theorem

It can be constructed a polygon only with the compass and the straight ruler, being sufficient that the number n of the polygon's sides to be a prime and to have an expression of the following form:

$n = f(m) = 2^{2^m} + 1$, where $m \in N$

Relations

a) $L_{2n} = \sqrt{2R(R - a_n)}$

$a_{2n} = \frac{1}{2}\sqrt{2R(R + a_n)}$

b) $L^2 + 4a^2 = 4R^2$

or

$L_{2n}^2 = R\left(2R - \sqrt{4R^2 - l_n^2}\right)$

$A_{2n}^2 = \frac{1}{4}R\left(2R + \sqrt{4R^2 - l_n^2}\right)$

where

$\frac{L}{l} = \frac{R}{a} = \frac{2R}{\sqrt{4R^2 - l^2}}$

l is the side of the inscribed polygon in O

L is the side of the circumscribed polygon in O

Equilateral triangle inscribed in the circle $C(O)$ and radius R

$L_3 = \sqrt{3}$

$a_3 = \frac{R}{2}$

$Aria_3 = \frac{l^2\sqrt{3}}{4} = \frac{3R^2\sqrt{3}}{4}$

$h = \frac{l\sqrt{3}}{2} = \frac{3R}{2}$

The hexagon inscribed in the circle $C(O)$ and radius R

$L_6 = R$

$a_6 = \frac{R\sqrt{3}}{2}$

$Aria_6 = \frac{p \cdot a}{2} = \frac{6R \cdot \frac{R\sqrt{3}}{2}}{2} = \frac{3R^2\sqrt{3}}{2}$

Geometric transformations

Measures:

a) Scalar (is a quantity): length, temperature, mass
b) Vectorial (size, direction, sense): speed, force

Vectors classification:

1) free – have an arbitrary position in space)
2) sliding – have the same line of support
3) Bound – have the same determined origin

Two vectors are equal if they have the same dimension, direction and sense.

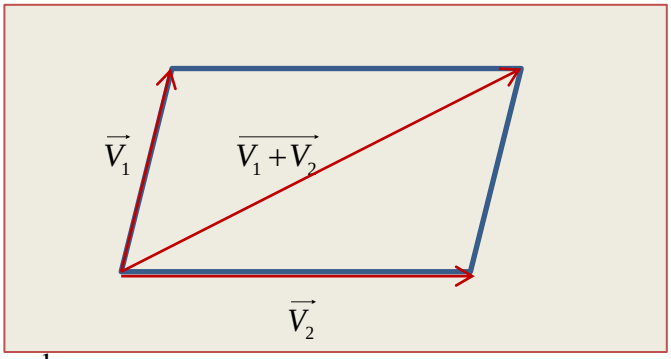
Properties:

a) Reflexive: $\overrightarrow{AB} = \overrightarrow{AB}$
b) Symmetric: if $\overrightarrow{AB} = \overrightarrow{CD} \Rightarrow \overrightarrow{CD} = \overrightarrow{AB}$
c) Transitive: if $\overrightarrow{AB} = \overrightarrow{CD}$ and $\overrightarrow{CD} = \overrightarrow{EF} \Rightarrow \overrightarrow{AB} = \overrightarrow{EF}$

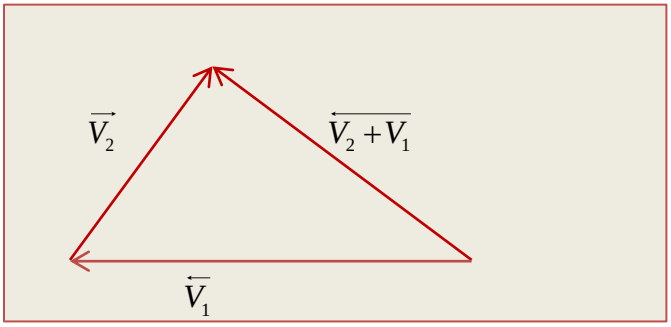
Vectors addition

To add two vectors we use the parallelogram's rule:

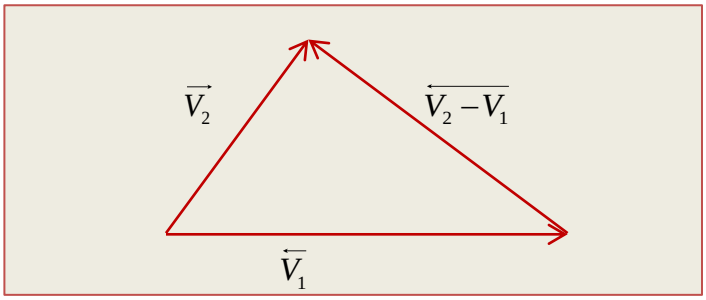
$$\left|\overrightarrow{V_1 + V_2}\right| \leq \left|\overrightarrow{V_1}\right| + \left|\overrightarrow{V_2}\right|$$



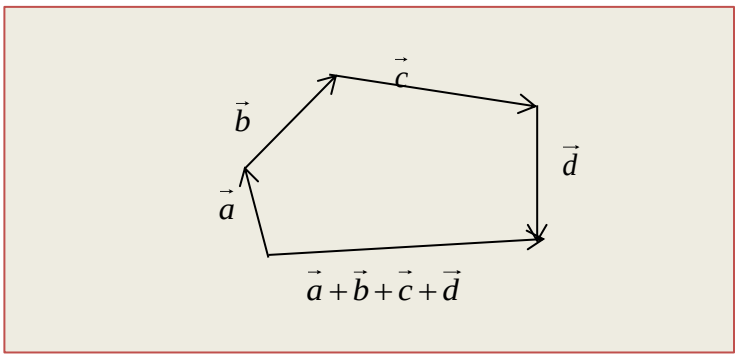
Or the triangle's rule



The difference of two vectors



To add several vectors it is used the polygon's rule: To sum any number of vectors we construct equal vectors with the given ones such that the origin of one coincides with the extremity of the next one. The vector whose origin coincides with the origin of the first vector, and the extremity coincides to the extremity of the last vector represents the sum of the given vectors.

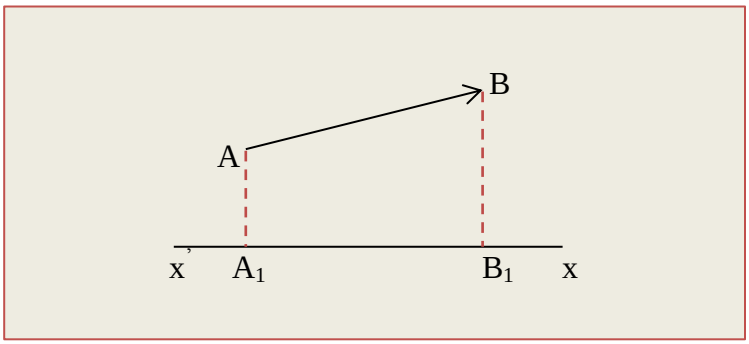


Multiplication of a vector with a number

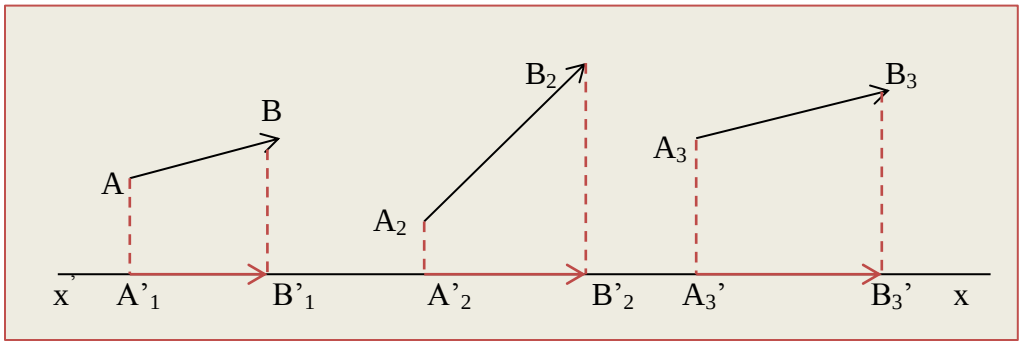
The product between a vector $\vec{a}$ and number λ is a vector whose module is equal to the product between the number's λ module and the module of vector $\vec{a}$, and whose sense is the sense of $\vec{a}$ or $-\vec{a}$, dependent of the sense of λ ($\lambda > 0$ or $\lambda < 0$). For $\lambda = 0$ the product is zero.

The projection of a vector on axis

The projection of a vector $\overrightarrow{AB}$ on the axis x is the size of vector $\overrightarrow{A_1B_1}$. It is denoted by pr. $_x\overrightarrow{AB}$.

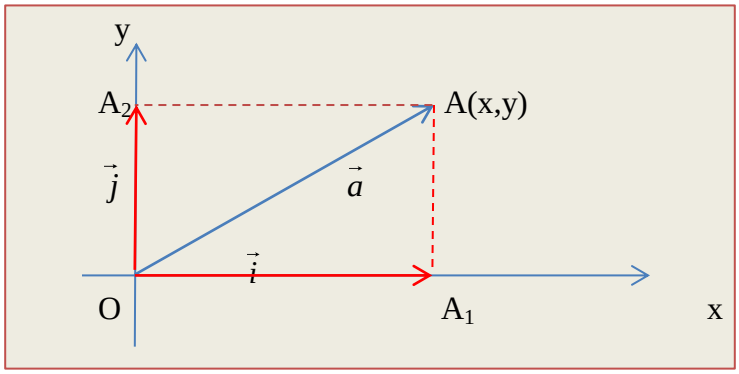


The projections of the vectors which have the same sense, on the same axis are proportional with their module.



$$\frac{A'_1B'_1}{\overrightarrow{A_1B_1}} = \frac{A'_2B'_2}{\overrightarrow{A_2B_2}} = \frac{A'_3B'_3}{\overrightarrow{A_3B_3}}$$

Decomposition of vectors in plane



$$\vec{a} = \overrightarrow{xi} + \overrightarrow{yj}$$

$\vec{i}$ and $\vec{j}$ are the axes' versors.

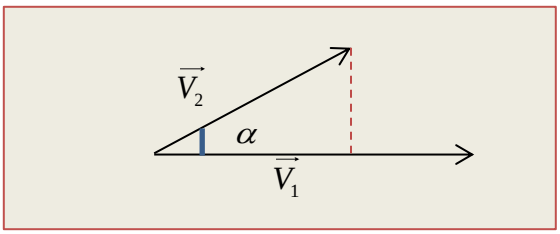
A versor or unit vector is the vector whose module is one (the unity).

The projection of vector sum on an axis is equal to the sum of the projections of the vector terms on the same axis.

The product of two vectors

The product of two vectors is equal to the product between their modules and the cosine of the angle formed by their directions.

$$\overrightarrow{V_1} \cdot \overrightarrow{V_2} = \left|\overrightarrow{V_1}\right| \cdot \left|\overrightarrow{V_2}\right| \cdot \cos\alpha = \overrightarrow{V_1} \cdot pr_{\overrightarrow{V_1}}\overrightarrow{V_2} = \overrightarrow{V_2} \cdot pr_{\overrightarrow{V_2}}\overrightarrow{V_1}$$



Translation

If to a point M in plane corresponds, through a certain rule (algebraic, geometric, mechanical, optical, etc.) a point M' well determined of the plan, we say that this correspondence defines a plane punctual transformation.

The plane translation defined by a vector $\vec{V}$ is the punctual transformation through which to each point A from plane corresponds a point A' from the plane such that $\overrightarrow{AA'} = \vec{V}$ (that is the segment AA' is equal, parallel and of the same sense with the oriented segment $\vec{V}$).

The translation is, therefore characterized by a vector and vice versa.

Through this transformation a figure F is transformed to an equal figure F' equal to it.

The translation conserves the lengths, angles (and the order of the points).

The set of translations form a group commutative.

Symmetry

The symmetry can be:

a) In relation to point
b) In relation to a line
c) In relation to a plane

The symmetry conserves the length and angles; transforms a figure F in an equal figure F' (its identical images)

Homothetic transformation

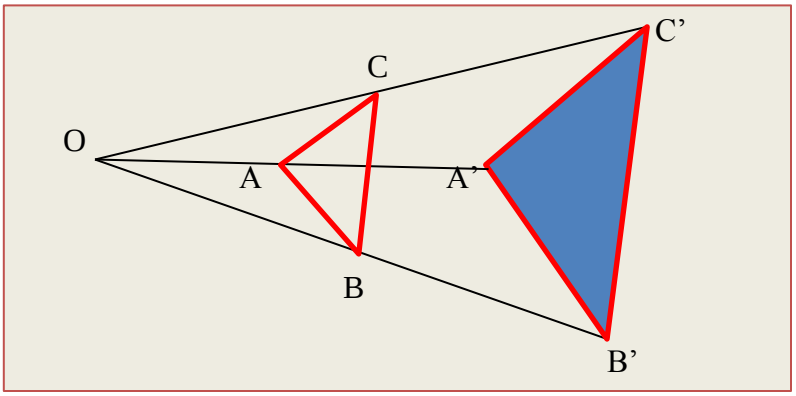
$$\frac{\overline{OC}}{\overline{OC'}} = \frac{\overline{OA}}{\overline{OA'}} = \frac{\overline{OB}}{\overline{OB'}} = ... = k$$

The point O is called the homothetic center of the homothetic transformation

F' is called the homothetic transformation of F

The homothetic transformation conserves the angles

k is the homothetic ration (here we have $k = \frac{2}{3}$)



Inversion transformation

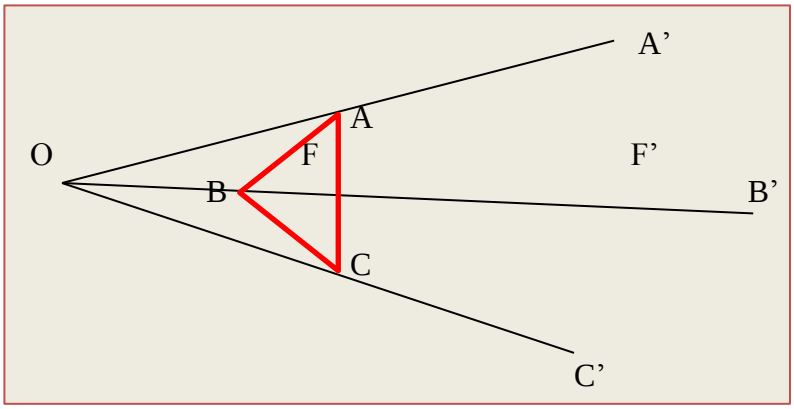
The inversion transformation conserves the angles

$$\overline{OA}\cdot\overline{OA'}=\overline{OB}\cdot\overline{OB'}=\overline{OC}\cdot\overline{OC'}=...=k$$

k is called the inversion power

The point O is called the inversion pole

F' is the inversion transformation of F



Rotation transformation

The rotation transformation of an angle α of the points in a plane in relation to a point (rotation center) is the punctual transformation which makes that to each point A of the plane to correspond a point A', such that $OA'=OA$ and $\sphericalangle AOA'=\alpha$ as measure and sense.

The rotation transformation conserves the lengths and the angles.

The rotation transforms a figure F to other equal figure F'

Conformal transformation

A conformal transformation is a succession of transformations that preserve the local angles.

Any segment constructed through the intersection point of the diagonals of a parallelogram and bordered by the parallel sides of the parallelogram is divided in two equal parts by this point.

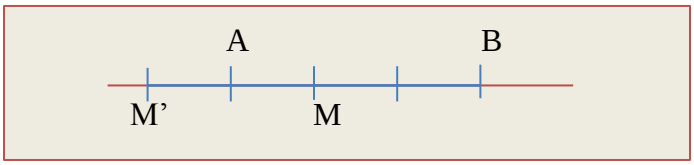
A line segment has as symmetry axis its perpendicular bisector.
An angle's symmetry axis is its bisector.
The isosceles triangle's axis of symmetry is its altitude.
The equilateral triangle has 3 axes of symmetry.
The rhombus has two axes of symmetry, these are its diagonals.
The rectangle has two axes of symmetry: the lines which connect the middle points of the opposite sides.
The parallelogram does not have any axis of symmetry.
The square has four axes of symmetry: two diagonals and the two segments that connect the middle points of the parallel sides.
The isosceles trapezoid has one axis of symmetry: the segment which connects the middle points of its bases.
The circle has an infinite number of axes (its diameters).

Proportional segments

Two segments are proportional with other two segments if the ratio of the first two is equal to the ratio of the other two segments.

The harmonic conjugate points

Two points are harmonic conjugate (one interior, the other exterior to a segment) when they divide this segment in the same ratio.



$$\frac{MA}{MB}=\frac{M'A}{M'B}=k$$

The points M',A,M,B form a harmonic division.

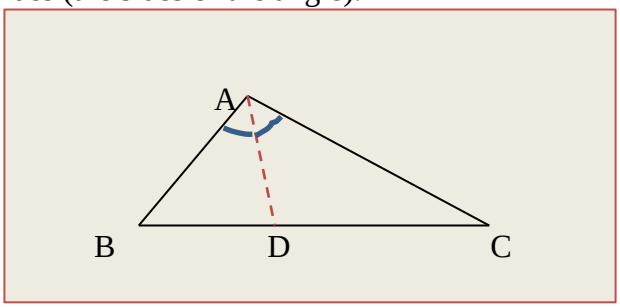
Thales' Theorem

In a triangle, a parallel to one of the sides will divide the other two sides in proportional segments.

Several parallel lines determine on two secant lines proportional segments.

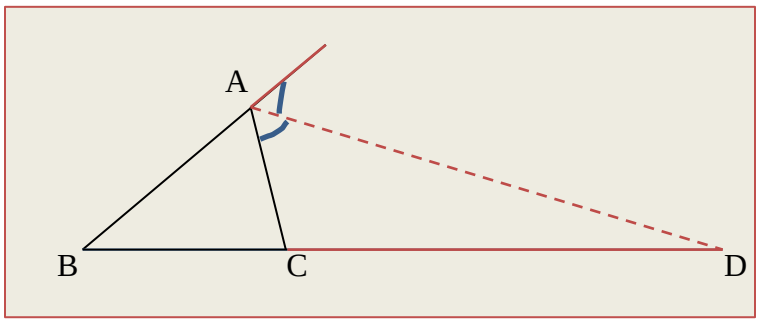
Bisector Theorem

Any bisector interior to a triangle divides the opposite side in proportional segments to the other sides (the sides of the angle).



$$\frac{BD}{DC} = \frac{AB}{AC}$$

Any exterior bisector of an angle of a triangle divides the opposite side of the triangle in proportional segments with the sides that form the angle.



$$\frac{BD}{CD} = \frac{AB}{AC}$$

Similarity of polygons

Two polygons with the same number of sides, whose angles are respectively equal, and the homological sides proportional are similar.

Homological sides are the sides which connect the vertexes of two angle respectively equal.

The cases of similarity of two triangles

Two triangles are similar if any of the following equivalent conditions occur:

1) If their angles are respectively equal
2) The homological sides are proportional
3) An angle equal between proportional sides.

The fundamental theorem of similarity

In a given triangle a parallel line to one of its sides forms with the other two sides a triangle similar to given triangle.

All equilateral triangles are similar.

The isosceles triangles which have the angle from the vertex equal or an angle from the base equal are similar.

The two right triangles, whose ratio of their hypotenuses is equal to the ratio of two catheti, are similar.

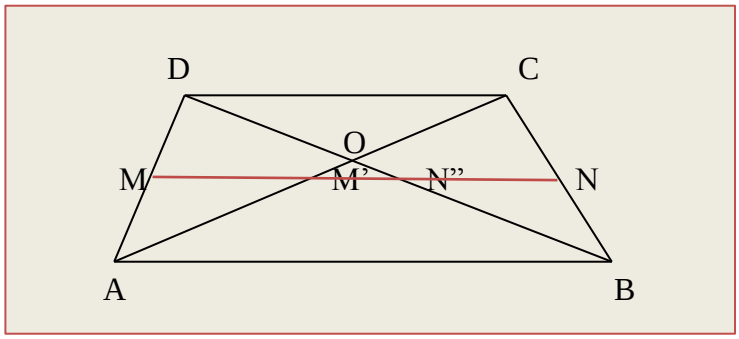
In a triangle ABC two cevians AA_1, AA_2 are isometric if the points A_1, A_2 are symmetric respective to the middle of the segment AB.

Proposition

The isotomic of three concurrent cevians are concurrent (Traian Lalescu).

The middle line of a triangle is the line segment which connects the middle points of two sides; it is parallel to the third line and equal to its half.

The middle line of a trapezoid is the line segment which connects the middle points of the non-parallel sides. It is equal to the half of the sum of the bases; it is parallel to the bases, being, therefore perpendicular on the middle of the height of the trapezoid.



MN is the middle line

$$MN = \frac{AB + CD}{2}$$

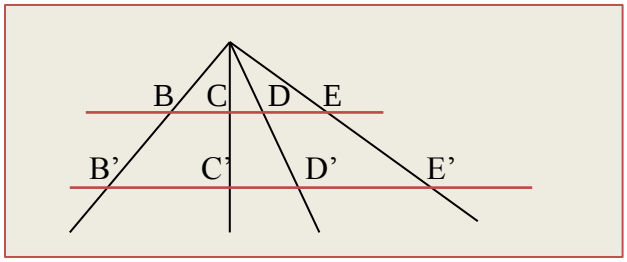
$$M'N' = \frac{AB - CD}{2}$$

Polar triangle

Polar triangle is the triangle formed by the feet of the perpendiculars constructed from a point on the sides of a triangle.

A fascicle of line determines on two parallel lines proportional segments.

$$\frac{BC}{B'C'} = \frac{CD}{C'D'} = \frac{DE}{D'E'}$$



The similarity ratio of two similar polygons is equal to the ratio of their perimeters.

Two similar polygons decompose in the same number of similar triangles, the same arranged.

Metric relations in a right triangle

The cathetus' theorem

In a right triangle a cathetus is the proportional average between the hypotenuse and its projection on the hypotenuse.

The altitude's theorem

In a right triangle, the altitude from the right angle is the proportional average between the segments determined on the hypotenuse.

Pythagoras Theorem

In a right triangle, the sum of the squared catheti is equal to the hypotenuse squared.

Conversely: If in a triangle the square of a side is equal to the sum of the square of the other two sides, then the triangle is a right triangle.

Pythagorean numbers – are the numbers which satisfy the Pythagoras' theorem

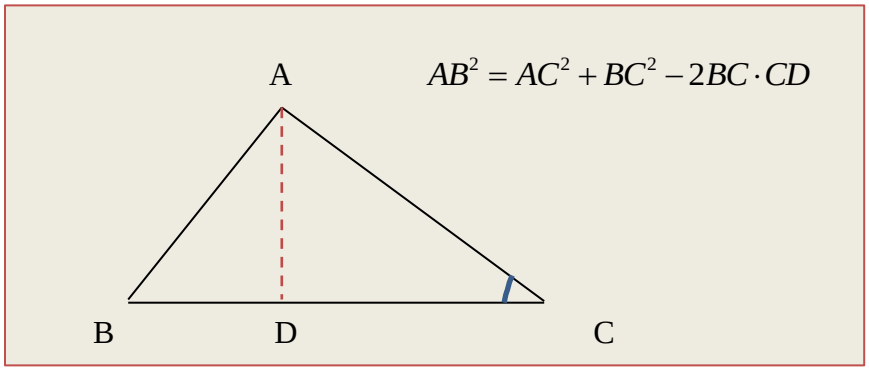
b	3	5	7	8	20	9	24	16
c	4	12	24	15	21	40	10	30
a	5	13	25	17	29	41	26	34

Metric relations in arbitrary triangles

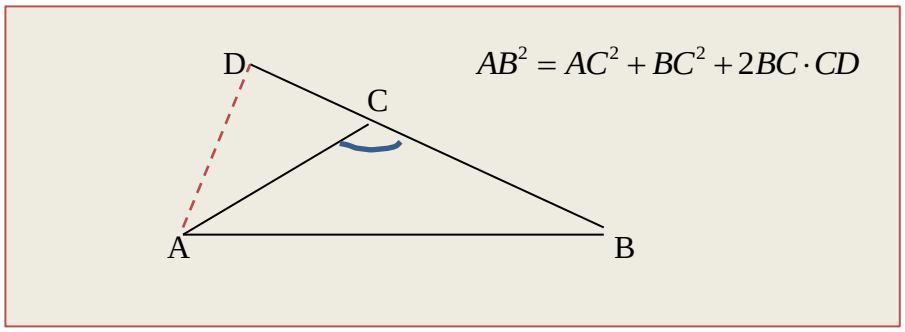
Generalized Pythagoras Theorem

In an arbitrary triangle the square of a side is equal to the sum of the square of the other sides to which is added or subtract twice the product between one side and the projection of the other side on it, depending of the angle opposed to the side is obtuse or acute.

Case I



Case II



Adjacent polygons

Adjacent polygons are the polygons which have one or more sides of line segments in common (without interior points in common).

Two equal polygons have equal area.

Two polygons which have the same area are called equivalent.

The ratio of the areas of two rectangles which have the same base is equal to the ratio of their height (altitudes).

The ratio of the areas of two rectangles is equal to the ratio between the products of their dimensions.

Heron (or Hero) Formula

$$S_{ABC} = \sqrt{p(p-a)(p-b)(p-c)}$$

where $p = \dfrac{a+b+c}{2}$

$$h_a = \frac{2}{a}\sqrt{p(p-a)(p-b)(p-c)}$$

$$\frac{1}{h_a} + \frac{1}{h_b} + \frac{1}{h_c} = \frac{1}{r}$$

$$\sin A \sin B \sin C = \frac{5}{2R^2}$$

$$r_a + r_b + r_c = 4R + r$$

$$\sin A + \sin B + \sin C = 4\cos\frac{A}{2}\cos\frac{B}{2}\cos\frac{C}{2}$$

$$tgA + tgB + tgC = tgAtgBtgC$$

Area of a rhombus

$$S_{Rhombus} = \frac{D \cdot d}{2} = L \cdot h$$

Area of a trapezoid

$$S_{Trapezoid} = \frac{(B+b)\cdot h}{2}$$

Aria of regular polygon

Aria of a regular polygon is equal to the semi product between the polygon's perimeter and its apothem

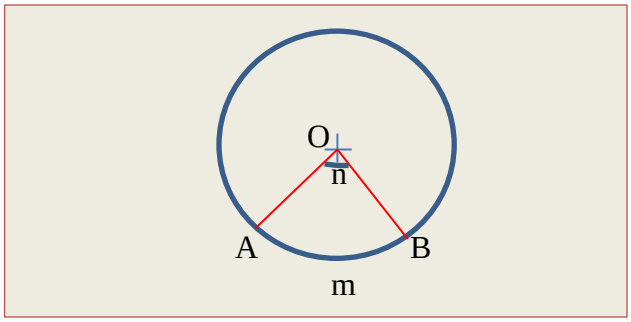
$$S = \frac{p \cdot a}{2}$$

Aria of a circle

$$S = \pi R^2$$

Aria of a circular sector

$$S = \frac{\pi R^2}{360} \cdot n = \frac{lenAmB \cdot R}{2}$$



The radius of a circle inscribed in a triangle is $r = \frac{S}{p}$, where S is the area of the triangle, and p is triangle's perimeter.

The radius of the circle circumscribed to a triangle is $R = \frac{abc}{4S}$, where a,b,c are the lengths of the triangle, and S is the area of the triangle.

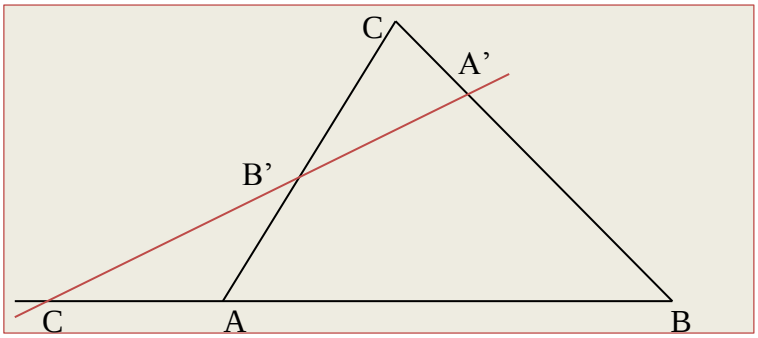
The ratio of the areas of two similar triangles is equal to the similarity ratio squared.

$$\frac{S}{S'} = \left(\frac{a}{a'}\right)^2$$

The ratio of the areas of two similar polygons is equal to the similarity ratio squared.

Menelaus' Theorem (Transversal's theorem)

If a line intersects the sides of a triangle ABC in the points A',B' and C', then between the segments determined on the sides of the triangle takes place the following relation



$$\frac{A'B}{A'C}\cdot\frac{B'C}{B'A}\cdot\frac{C'A}{C'B}=1$$

Converse:

If two points are on the triangle's sides and the third on the extension of the third side of the triangle, or all the points are on the extensions of the sides of the triangle.

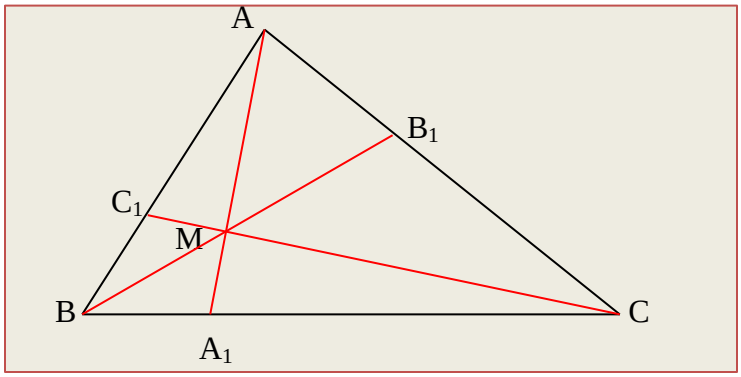
The generalization of Menelaus's theorem (Carnot)

If a line intersects the sides A_i,A_{i+1} of a polygon in M_i, then

$$\frac{M_1A_1}{M_1A_2}\cdot\frac{M_2A_2}{M_2A_3}\cdot\frac{M_3A_3}{M_3A_4}\cdot\ldots\cdot\frac{M_nA_n}{M_nA_1}=1$$

Ceva's theorem

If through the vertexes of a triangle we'll construct three concurrent cevians AA_1,BB_1,CC_1, then between the segments determined by the points A_1,B_1,C_1 on the opposite sides takes place the following relation:



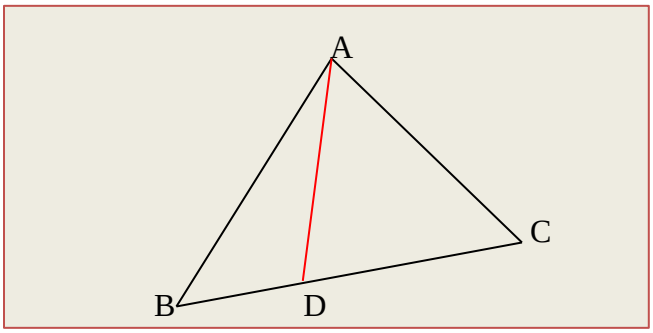
$$\frac{A_1B}{A_1C}\cdot\frac{B_1C}{B_1A}\cdot\frac{C_1A}{C_1B}=-1$$

$$M\in\mathcal{P}(ABC)$$

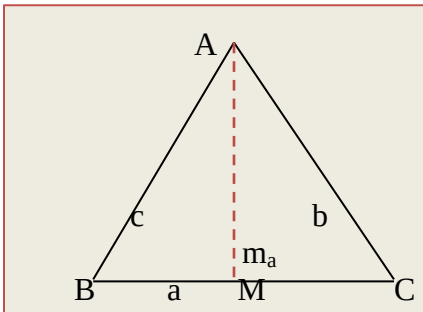
Van Aubel's theorem

In a triangle ABC, let D a point on BC. Between the points D, and B,C takes place the following relation:

$$AB^2\cdot DC+AC^2\cdot BD-AD^2\cdot BC=BC\cdot BD\cdot CD$$



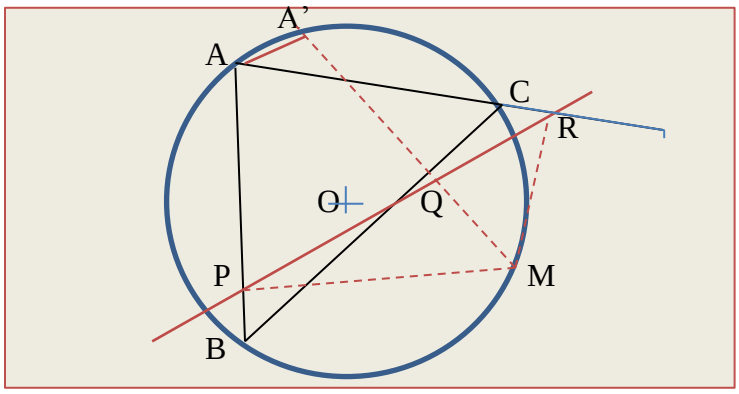
The median's theorem



$$(m_a)^2=\frac{2(b^2+c^2)-a^2}{4}$$

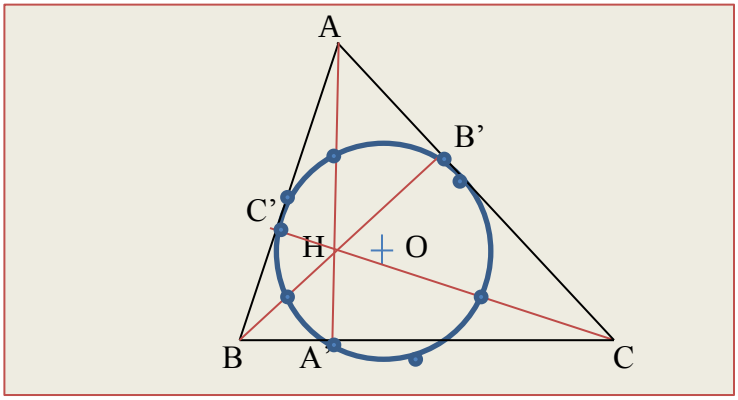
Simson's line

Let ABC a triangle inscribed in a circle and M a point on the circle. The points of the intersection of the perpendiculars constructed from M on the sides of the triangle are three collinear points P,Q,R. The line is called Simson's line



If A' is the intersection of the point M on BC, as above then AA' is parallel with the Simson's line PQR.

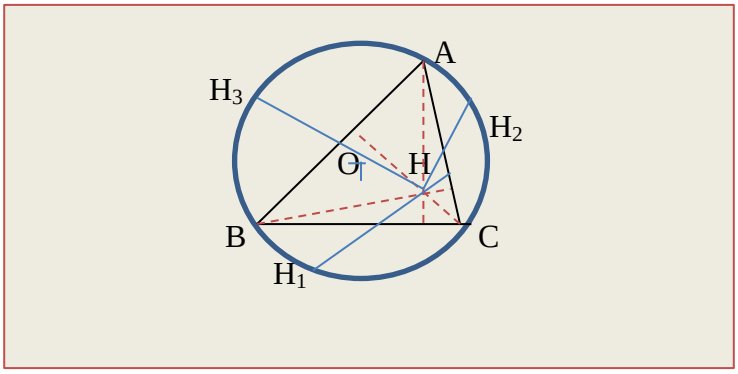
Euler's circle (the circle of the 9 points)



In a triangle, the points where the heights of the triangle intersect, the middle points of the middle of the sides of the given triangle and the middle of the segments AH, BH, CH .are situated on a circle.

The center of direct homothety of the circumscribed and that of the circle of the 0 points is the orthocenter H, and the homothety ration is equal to $\frac{1}{2}$.

Euler's Theorem



The symmetric of the orthocenter in relation to the middle points of the sides are on the center of the triangle's circumscribed circle.

Isogonal lines

Isogonal lines are two lines which pass through the vertex of an angle and form angles equal with the sides of the triangle (are symmetric in rapport to the angle's bisector.

Symmedian

Symmedian is the median's isogonal (the line that connects the vertex with the intersection of the tangents at the edge of the opposite side).

The point of Lemoine

The three symmedians of a triangle are concurrent in appoint called the Lemoine's point –it is isogonal to the center of mass of the triangle.

The distances from the point of Lemoine to the sides of the triangle are proportional.

Antiparallel lines

Two lines AB,CD are antiparallel with respect with the sides of an angle XOY, if angle OAB of the first line with OX is equal to the angle OCD made by the second line with OY.

Two vertexes of a triangle, the center of the inscribed circle I and the center of the ex-inscribed circle of the triangle I_a are on a circle whose diameter is II_a, with the center in the middle or the arc BC of the circumscribed circle. A side BC is viewed from the center I of the inscribed circle under an angle of $90°+\frac{A}{2}$ and from the center I_a of the ex-inscribed circle under an angle of $90°-\frac{A}{2}$.

The cevian of rank k

The cevian of rank k is the line AD with the property that $\frac{BD}{CD}=\left(\frac{c}{b}\right)^k$.

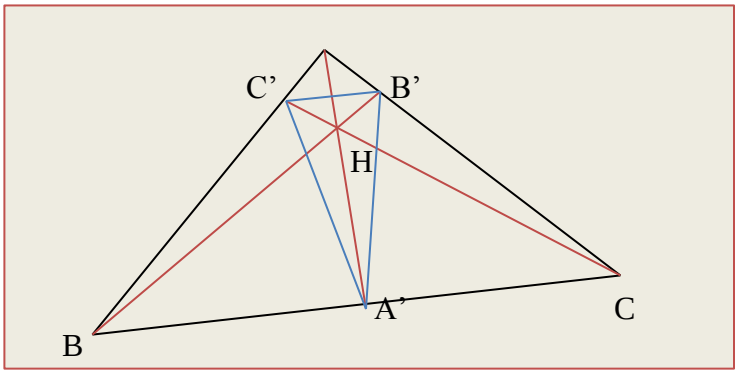
The median = the cevian of rank 0, bisector of rang 1, symmedian of rank 2

The cevians of rank k are concurrent.

If a quadrilateral is circumscribed to a circle, the sum of two opposite sides is equal to the sum of the other two sides and conversely.

The circle which passes through the points B,C and through the orthocenter H of a triangle is the symmetric of the circumscribed circle of the triangle with respect to the side BC.

Orthic triangle

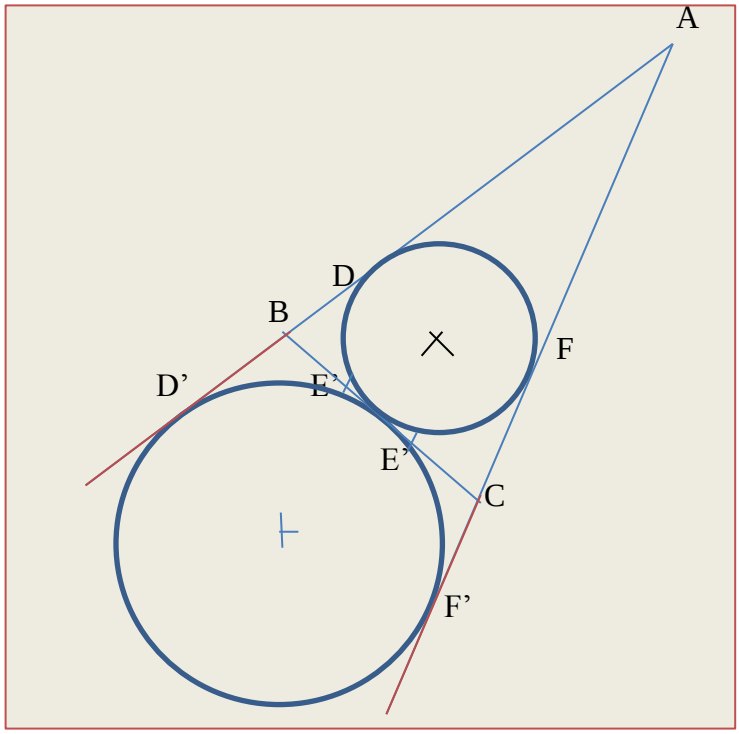


The altitudes of a triangle ABC are bisectors for the triangle orthic $\sphericalangle B'A'C' = 180° - 2A$; the perpendiculars from the vertexes of triangle ABC on the sides of the orthic triangle $A'B'C'$ are concurrent in the center of the circumscribed circle to triangle ABC.

The distance from a vertex A to the orthocenter is twice the distance from the center of the circumscribed circle to triangle ABC o the opposite side.

The symmetric of the orthocenter relative to the middle of the sides are on the circumscribed circle; the segments HA_1 (A_1 diametric opposed to A) and intersect in the middle.

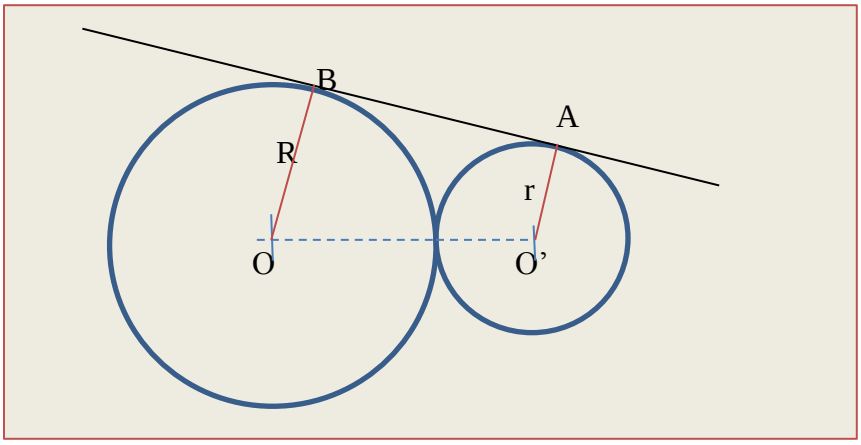
The inscribed triangle ABC - sides a,b,c and perimeter p - touches the sides in the points D,E,F; the ex-inscribed circle in the angle BAC touches the sides in D',E',F'; $AE' = AF' = p$, $AE = AF = p - a$; $BD = BF = CD' = CE' = p - b$



The radiuses of the circles inscribed and ex-inscribed of a write angle triangle are $r = p - a,\ r_a = p,\ r_b = p - c,\ r_c = p - b$

The product of the sides of a triangle is equal to twice the product between the triangle's aria and the diameter of the circumscribed circle $abc = 2Sd$.

The length of the common tangent of two tangent circles is twice of the geometric average of their radiuses: $abc = 2\sqrt{R \cdot r}$



Orthogonal circles

The circles which intersect forming an angle of 90 (that is the tangents to the circles constructed in one of the common points are perpendicular)

$$d^2 - r^2 + r'^2$$

where d is the distance between the centers of the two circles, r and r' are radiuses of the two circles.

The power of a circle whose radius r to an orthogonal circle to is r^2, and conversely.

The circles with the centers on the same line and which have the same radical axis form a fascicle. There is an infinity of circles with the centers of orthogonal axis, orthogonal to the circles in a fascicle; these form a conjugate fascicle to the given fascicle.

Two circles are twice homothetic.

d'Alembert theorem

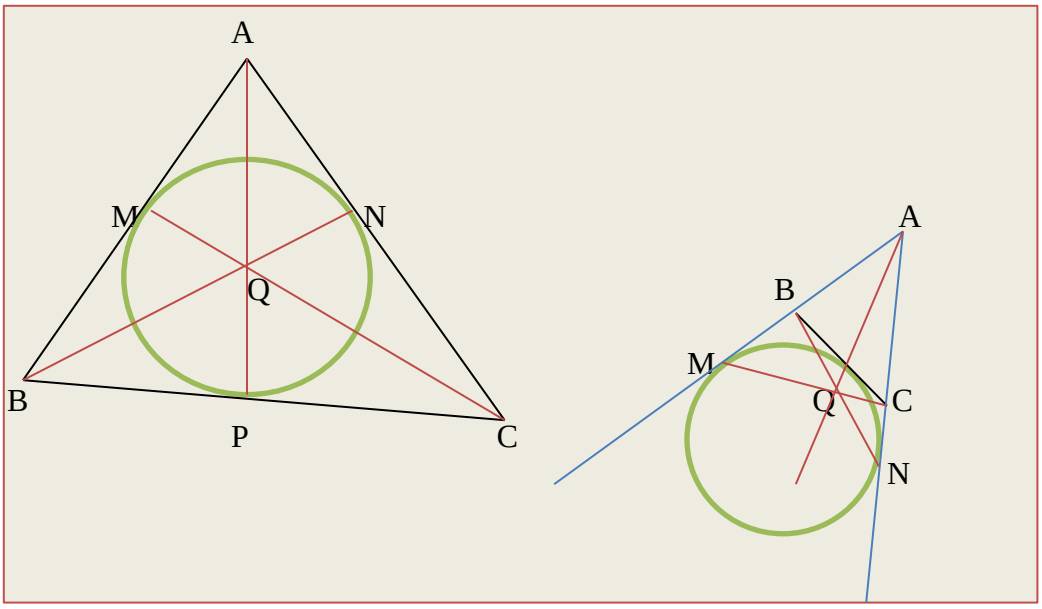
The centers of a direct homothety of three circles taken two by two, are collinear; a center of direct homothety and two of inverse homothety are collinear.

Gergonne's theorem

The lines which connect the vertexes of a triangle with the contact points of the inscribed circle on the opposite sides are concurrent.

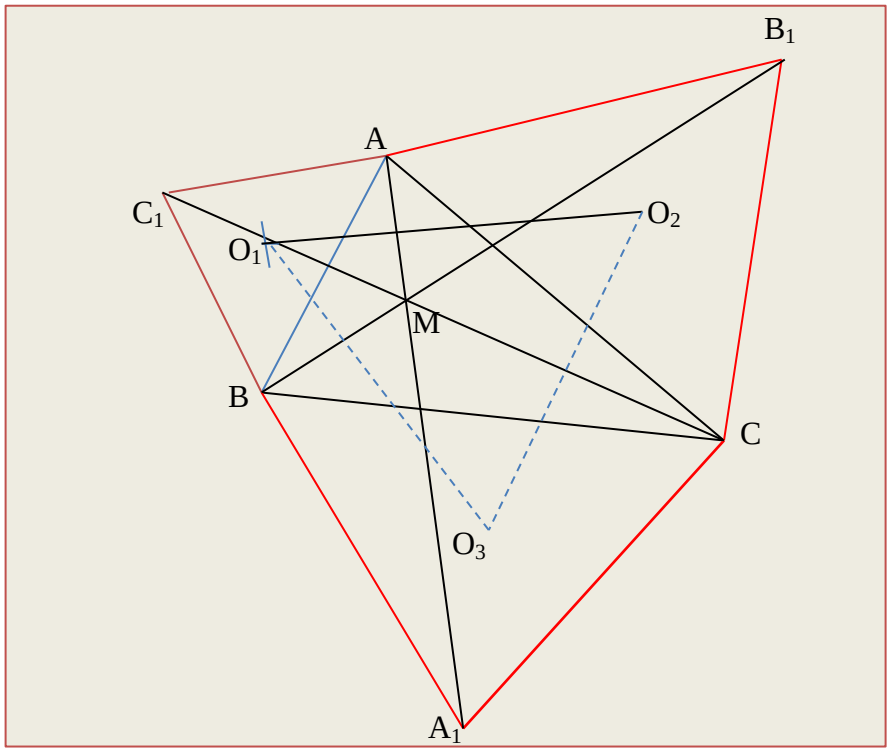
$$AP \bigcap BN \bigcap CM = Q$$

Conversely we can say about the lines which connect the vertexes of a triangle with the contact points of the circle ex-inscribed



Torricelli's theorem

If on the sides of a triangle ABC we'll construct equilateral triangles in exterior)or all in interior)l the lines AA_1, BB_1, CC_1, which connect the vertexes of the given triangle to the corresponding vertexes of the equilateral triangles, are equal and concurrent in a point M.



The circle BCA_1, and the similar ones pass through M; the sides of the triangle are viewed under equal angels from M; the centers of the equilateral triangles form an equilateral triangle. If M is in the interior of the given triangle, then $MA+MB+MC$ is minimum.

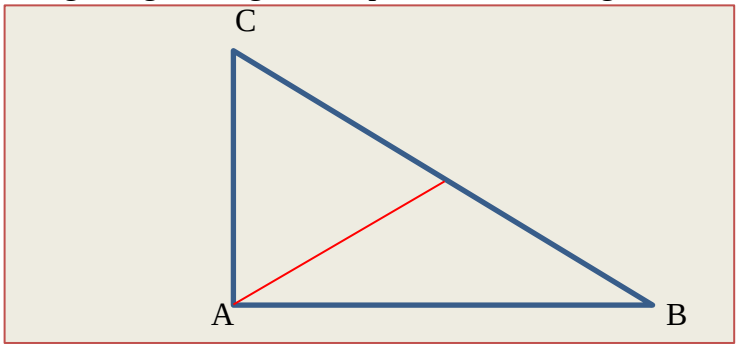
M is called Torricelli's point, and the concurrent circle are called the Torricelli's circles
$O_1O_2O_3$ is the Napoleon triangle

$$O_1O_2 = \frac{a^2+b^2+c^2+4S\sqrt{3}}{6}$$

$$O'_1O'_2 = \frac{a^2+b^2+c^2-4S\sqrt{3}}{6}$$

The relation of Van Aubel

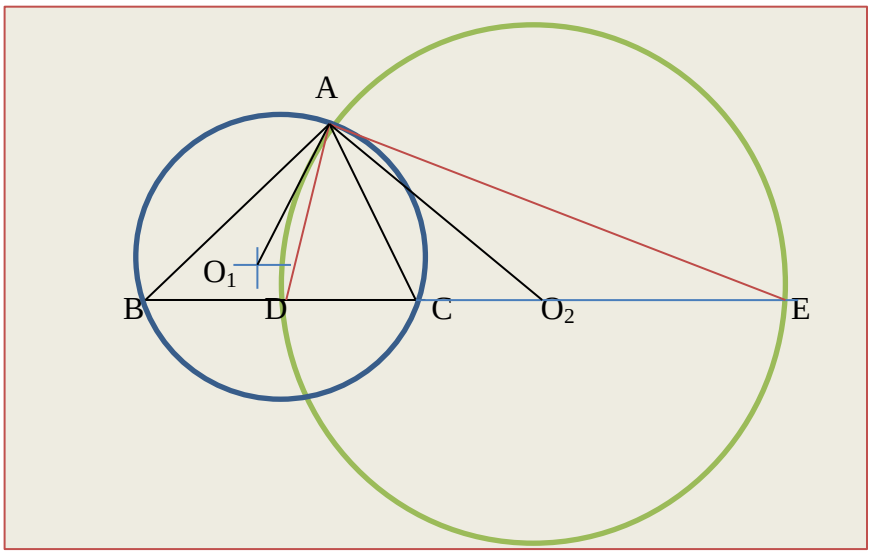
In a right angle triangle takes place the following relation



$$AB^2 \cdot MC^2 + AC^2 \cdot MB^2 = BC^2 \cdot MA^2$$

Apollonius circle

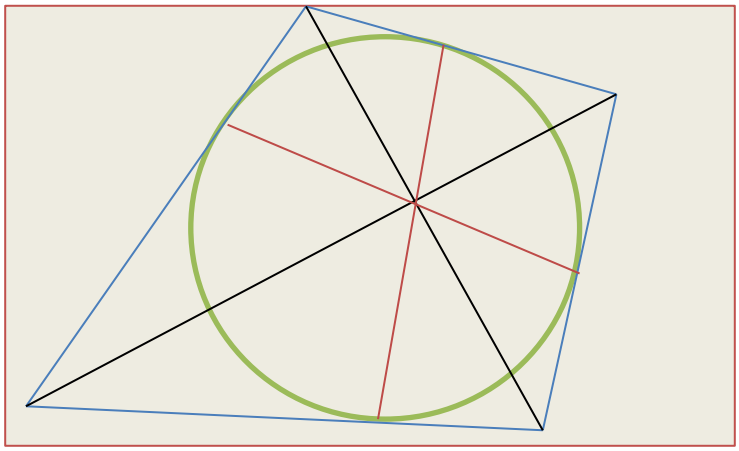
The circle whose diameter is the segment DE formed by the legs of the bisectors of angle A on the opposite side is orthogonal to the circle circumscribed to triangle ABC.



The center of the Apollonius circle is at the intersection of the tangent from vertex A with the side BC. The ratio of the distances of the point of the Apollonius circle to the vertexes B,C is constant and equal to $\frac{AB}{AC}$.

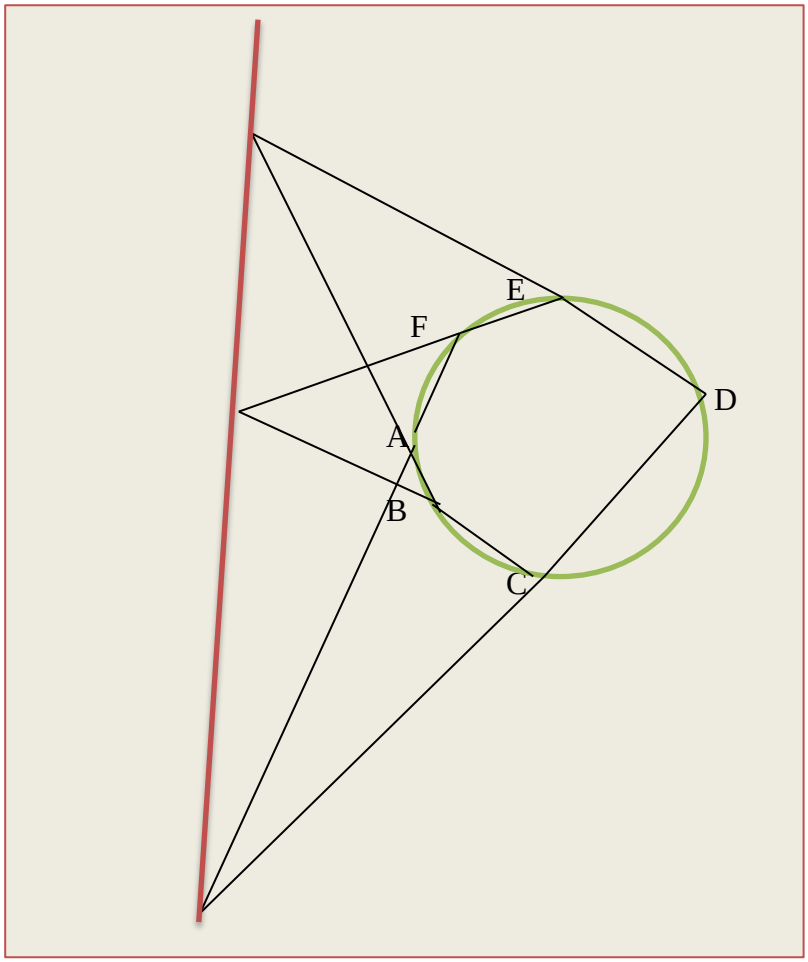
Newton's theorem

In a circumscribed quadrilateral, the diagonals and the lines which connect the contact points of the opposite sides are concurrent



Pascal's theorem

The opposite sides of an inscribed hexagon intersect in collinear points.



Miquel's point

The circumscribed circles to the triangles formed by four lines (complete quadrilateral) have a common point.

The centers of these circles and the Miquel's point are on the circle.

The Lemoine line

The symmedians of a triangle are concurrent (the Lemoine's point). The symmedian divides the opposite line in the ratio of the adjacent sides.

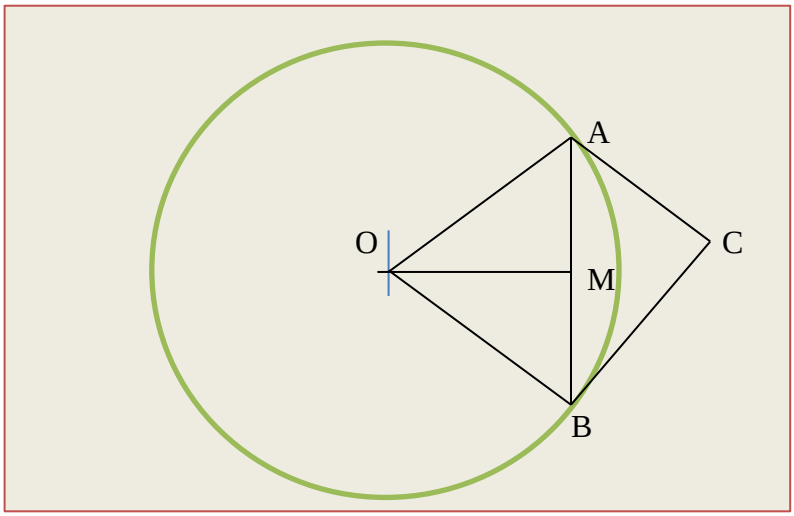
The tangent in a vertex of the triangle is conjugated to the symmedian; divides the opposite sides in the same ratio.

The points of intersection of the tangents with the opposite sides are situated on a line called Lemoine line.

In a right angle triangle the symmedian of the right triangle coincide with the altitude and the Lemoine's point with the middle point of this altitude.

The distances of the Lemoine's point to the sides are proportional to the triangle's sides.

An adjoin circle $\overline{AB}$ is the circle that passes through A and is tangent in B to the side BC of a triangle.



Brocard theorem

The adjoin circles $\overline{AB}, \overline{BC}, \overline{CA},$ are concurrent.

The circles $\overline{BA}, \overline{CB}, \overline{AC}$ are concurrent (the first point of Brocard (retrograde point).

The point of Nagel: The lines which connect the vertex of a triangle with the contact points on the opposite sides of the ex-inscribed circles are concurrent. The points N, G, I are collinear.

Quadrilateral harmonic

The product of two opposite sides is equal to the product of the other opposite sides (quadrilateral inscribable); this equality takes place when the vertices A,B,C,D are in a harmonic ratio (e.g. M being arbitrary on a circle, the fascicle $M(ABCD) = -1$.

A mobile tangent sections four fixed tangents in a given harmonic ratio.

The locus of the conjugates of a point M on a mobile secant constructed through M, in relation to the ends of the determined cord, is a line, called the polar of M, perpendicular on the diameter of the point M. The pole of a tangent is the contact point. The pole of a secant is the intersection of the tangents in the points of the intersection with the circle.

The polar of three collinear points are three concurrent lines, and conversely.

If a line d passes through the pole of a line d', the property is converse The lines d and d' are called conjugate.

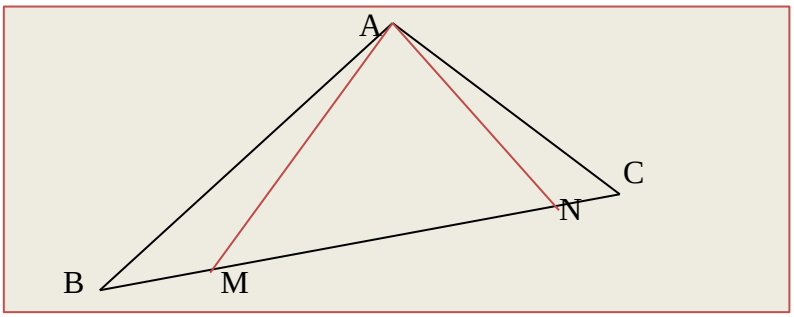
To any figure formed of points and lines corresponds to figure called the dual – formed of lines (the polar of the points) and of the points (the lines pole).

Pappus' theorem

We divide the sides $\overline{BC}, \overline{CA}, \overline{AB}$ of a triangle in the same ratio, through the points M, N, P. The triangle MNP has the same mass center as the given triangle ABC.

Steiner's theorem

Through the vertex A of a triangle, we construct two isogonal cevians, which intersect the side BC in M, N. Then the following relation takes place:



$$\frac{CM}{BM}\cdot\frac{CN}{BN}=\frac{AC^2}{AB^2}$$

Pompeiu's theorem

If the triangle ABC is equilateral and we take a point P which belongs to the plane $P(ABC)$, then the lines PA, PB, PC can determine a triangle. If $P\in\mathcal{C}(A,B,C)$ then the triangle is degenerate (the sum of two sides is equal to the third side)

Generalization (Viorel Gh. Vodă)

$PA\sin A, PB\sin C$ form a random triangle.

The tangents to a circle constructed from the ends of two perpendicular cords form an inscribable quadrilateral.

The tangent in A to the circle ABC is parallel to the line $B'C'$, which is the line obtained by connecting the legs of the altitudes from B, C.

The Geometric locus of the middle point M_1 of segment AM, when A is fixed and M describes a given circle, is a circle od radius $r=\frac{R}{2}$ of whose center is on the middle of the segment OA (O is the center of the circle described by M; R is the radius of this circle).

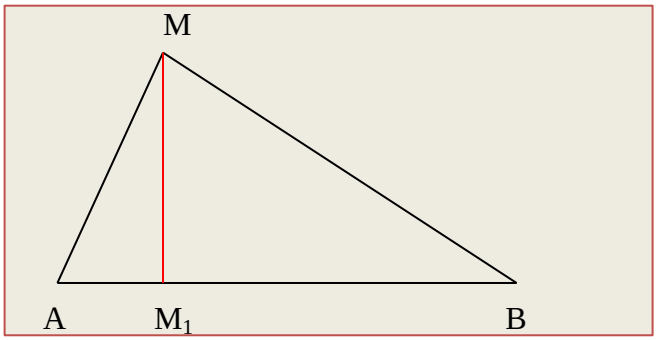
The geometric locus of the center of the inscribed circle to the triangle ABC when B,C are fixed and A is mobile on the circumscribed circle to the triangle ABC is an arc of $90°+\frac{A}{2}$.

Homological triangles

If the lines AA_1,BB_1,CC_1 are concurrent, then the triangles ABC and $A_1B_1C_1$ are called homological. If $BC\cap B_1C_1=\alpha$, $CA\cap C_1A_1=\beta$, $AB\cap A_1B_1=\gamma$, then the points α,β,γ are collinear (Desargues' theorem) (the Gergonne point). (The generalization is not true.)

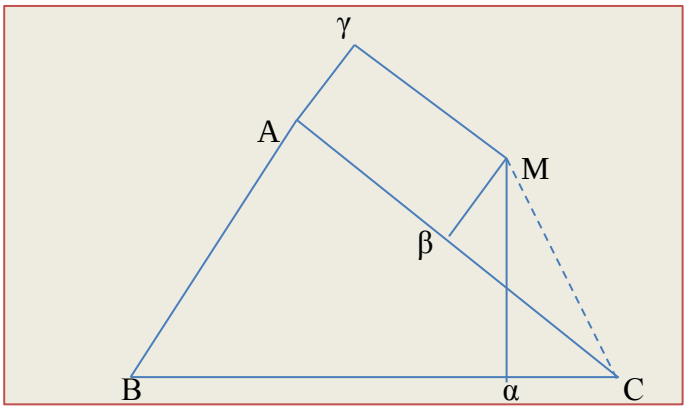
The sum of the squared sides of a parallelogram is equal to the sum of its squared diagonals.

In a random triangle, MM_1 being the altitude, takes place the following relation:



$$MA^2-MB^2=M_1A^2-M_1B^2$$

If the projections of a point M on the sides of a triangle ABC are α,β,γ, takes place the following relation:



$$B\alpha^2-C\alpha^2+C\beta^2-A\beta^2+A\gamma^2-B\gamma^2=0$$

The orthopole theorem

Let a triangle ABC and a line (d), let A',B',C' the projections of the vertexes A,B,C on (d). The perpendicular from A' on BC and the analogues are three concurrent lines [the concurrency point is called the line's orthopole to respect to the triangle (the Neuberg's point)].

Feuerbach theorem

The circle of the nine points is tangent to the inscribed and ex-inscribed circles.

Geodesic

A geodesic is the smallest length between two points on a surface.

$\frac{1}{r}=\frac{1}{h_a}+\frac{1}{h_b}+\frac{1}{h_c}$ (r is the radius of the inscribed circle, h_a is the altitude from point A.

The by-ratio of four points non collinear M_1,M_2,M_3,M_4; $\frac{\overline{M_3M_1}}{\overline{M_3M_2}}:\frac{\overline{M_4M_1}}{\overline{M_4M_2}}$

If $R=-1$, then the by-ratio is harmonic.

Bretschneider's theorem

In a convex quadrilateral $ABCD$ takes place the following relation:

$$d_1^{\,2}d_2^{\,2}=a^2c^2+b^2d^2-2abcd\cos(A+C)$$

Chapter Three: Spa□ e Geo□ etry

The fundamental elements of space geometry

a) The point $(A,B,C,...)$
b) The line $(a,b,c,...)$
c) The plane $(\alpha,\beta,\gamma,...)$

Definition
The position relations are the relations between the fundamental elements.

Definition
A geometric figure is formed of points, lines, or planes.
Figures can be:
1. Plane, which are figures that can be entirely laid (with all points) on a plane
2. In space, which cannot be laid entirely (with all points) on a plane

The axioms of space geometry

1. Three non-collinear points determine a plane.
2. If two points of a line are on a plane, then the line is entirely contained in that plane.
3. If two planes have a common point, then these have at least one more point in common.
4. In a space there exist at least four non-coplanar points (which are not on the same plane).

Theorem
Two distinct planes, which have a common point, intersect by a line that passes through that point. (The intersection of two distinct planes is a line).

Determination of a plane

a) Three non-collinear points;
b) A line and an exterior point;
c) Two concurrent lines;
d) Two parallel lines.
e) The mobile lines which pass through a point and are supported on a fixed line
f) Mobile lines that are supported on two concurrent lines
g) Mobile lines that are supported on two parallel lines
h) Mobile lines that are supported on a line and are parallel with another line.

The positions of a point with respect to a plane

a) The point is on the plane;
b) The point is exterior of the plane.

The relative positions of two lines

a) Concurrent;

b) Parallel
c) Coincide
d) Arbitrary

Euclid Postulate

Through a given point we can construct only one parallel line to the given line (this is true in the plane geometry as well as in the space geometry).

Theorem

Two lines parallel to a third line are parallel.

Theorem

Two planes which have a common point and which contain two parallel lines respectively intersect in a line which is parallel with the two given parallel lines.

Theorem

Two angles, that are not on the same plane, and which have their sides parallel, are equal.

Theorem

If a line is parallel to plane, the parallel to the given line constructed through a point of the plane it will be contained in the plane.

Definition

A line in a plane divides it in two regions called semi-planes.

Definition

A plane separates the space in two regions; to pass from a region to the other, the plane must be traversed. These regions are called semi-spaces.

Theorem

If two lines are parallel, any plane which intersects one of them will intersect the second line also.

Theorem

A line which is parallel to two planes is parallel with their intersection.

Theorem

Through an exterior point of a plane one can construct an infinity of parallel lines to the given plane; all these lines being situated in the plane which is parallel to the given plane constructed through the exterior point

Definition

The angle of two semi-lines in space is defined as the angle whose vertex is a random point and the sides are parallel and oriented in the same sense as the given semi-lines.

The relative positions of the line in relation to a plane

a) The line parallel with the plane;
b) The line intersects the plane in a point. The line is contained in the plane.

Theorem

If a line is parallel with a line contained in a plane, it is parallel with the plane.

Theorem

If a line is parallel with a plane, the intersection of a plane constructed through the line with the given plane is parallel line to the given line.

Theorem

If two planes have a common point and are parallel with the same line, then their intersection is parallel with this line.

Theorem

If two lines are situated such that any plane which intersects one of them, intersects the second also, their intersection is parallel to this line.

Theorem

The parallel lines to two secant lines of a plane, constructed through an exterior point of the plane, determine a plane parallel to the given plane.

Definition

A class is a subset of all the elements that satisfy the following properties:

a) Symmetry: if $a \| b$ then $b \| a$;
b) Transitivity: If $a \| b$ and $b \| c$, then $a \| c$.

Definition

The elements of a class are equivalent with respect to the defined relation, which is called relation of equivalence.

Examples of relations of equivalence:

1) The relation of equality
2) The similarity relation

Theorem

All parallel lines between them have the same direction (a line is parallel to itself)

Theorem

The middle points of the sides of a quadrilateral form a parallelogram.

Theorem

If a plane is parallel to the intersection of two planes, then all planes intersections are parallel by two.

Theorem

A line is perpendicular on a plane if it is perpendicular on all the lines of that plane.

Theorem

If a line is perpendicular on two lines of a plane, which are not parallel, then it is perpendicular on all of the lines of the plane, therefore it is perpendicular on the plane.

Theorem

In a point of a line it can be constructed an infinity of perpendicular lines on the given line; all these perpendicular lines are contained in a plane which is perpendicular on the line in that point (called normal plan of the line in the given point).

Therefore, in a point of a line we can construct only one perpendicular plane on that line.

Theorem

Through a point we can construct only one perpendicular line on a plane.

Theorem

Any parallel line to a perpendicular line on a plane is perpendicular on the plan.

Theorem

Two perpendicular lines on the same plane are parallel lines.

Theorem

A line and a plane perpendicular on the same line are parallel.

Theorem

From a point exterior to a plane it can be constructed only one perpendicular line on a plane and multiple oblique lines.

Theorem

The perpendicular line is shorter than any oblique line.

Theorem

Two oblique lines, whose legs are at an equal distance from the leg of the perpendicular, are equal.

Theorem

From the oblique lines, the shortest is that whose leg is closest to the perpendicular line's leg.

Theorem

If two oblique lines constructed from the same point on the same plane are equal, then their legs are at equal distance from the perpendicular line's leg; between two unequal oblique lines, the leg of the shortest is the closest to the perpendicular line's leg.

Symmetry (Punctual transformation)

a) Symmetry with respect to a point (central)
b) Symmetry with respect to a line
c) Symmetry with respect to a plane

Theorem

Two symmetric figures are equal; if the distances of the homological points are equal, but the figures cannot overlap, it results that these are invers equal.

The theorem of the three perpendiculars

If from point A of plane P is constructed a perpendicular line AB on the plane and the perpendicular line AC on a line (D) from the plane, then the line which connects the point C with a random point on the line AB is perpendicular on (D).

Converse I

If from the point B, exterior to plane P, is constructed a perpendicular BA on the plane and the perpendicular BC on line (D) from the plane, then the line AC which connects the legs of the two perpendiculars constructed from B is perpendicular on (D).

Converse II

If in the point C of the line (D) from the plane P are constructed two perpendiculars on it, namely CA in plane and CB exterior, then the perpendicular constructed from a point of CB on CA is perpendicular on the plane.

Theorem

The set of points at an equal distance from two given points is called the mediator plane of the segment formed by the two given points.

Theorem

The set of points at equal distance of three given non-collinear points is a perpendicular line on the triangle's plane formed by the given three points, in the center of the circumscribed circle of the triangle.

Theorem

With respect to four non-coplanar points there exists only one point situated at equal distance from them.

Theorem

The set of points of a plane for which the ratio of the distances to two points is constant is a circle with the center on the line determined by the given two points (The circle of Apollonius).

The relative positions of two planes

a) Parallel
b) Intersect
c) Identical

Theorem
Two planes perpendicular on the same line are parallel.

Theorem
If two concurrent lines in a plane are respectively parallel with two lines from another plane, then the two planes are parallel.

Theorem
If two lines concurrent in a plane are parallel with another plane, then the two planes are parallel.

Theorem
Through an exterior point exterior to a plane it can be constructed only one plane parallel to the given plane.

Theorem
The intersections of two parallel planes through a third plane are parallel lines.

Theorem
Two parallel planes to a third plane are parallel.

Theorem
If two planes are parallel, then any line perpendicular on one of the planes will be perpendicular on the second plane also.

Theorem
The parallel line segments between parallel planes are equal.

Theorem
The distance from a point in a plane to another plane is the distance between the planes.

Theorem
Multiple parallel planes determine on a fascicle of lines proportional segments.

Theorem
If two planes are parallel, then any line which intersects one of them will intersect the second as well.

Theorem
The set of points which are at an equal distance from a plane consists of two parallel planes to the given plane, which are situated on both sides of the plane at the given distance.

Theorem
The set of points at an equal distance from two parallel planes is a parallel plane to the given planes at an equal distance (equidistant plane)

Theorem

Through a point of a line it can be constructed only one plane perpendicular on that line.

Translation

Theorem

The segments which correspond through a translation are equal and parallel.

The translation transforms a figure to another equal figure which is parallel to the given figure; in particular transforms a line into another line, and a plane to another plane.

Definition

Parallel figures are the figures which have the property that the homological sides are parallel.

Rotation

Theorem

In a rotation around a line, the distance between two random points does not change.

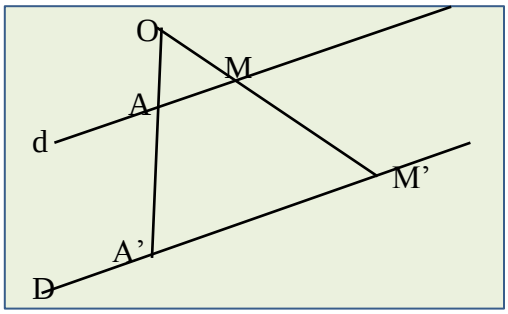
Theorem

Through a rotation a figure is transformed into an equal figure; in particular, a line is transformed into a line, a plane is transformed into a plane.

Homothety

Definition

The homothetic center (O) is the point with respect to which is executed the punctual transformation.



$\frac{OM'}{OM} = \frac{OA'}{OA}k$, where k is the ratio between the distances from the center (O) to the homological points of the figure.

The homothetic of a figure f is the figure which is obtained through the transformation.

Theorem
The homothetic of a line is a line parallel to the given line.

Theorem
The homothetic of a plane is a plane.

Theorem
In a homothety two homological segments are in the same ratio.

Theorem
The figures obtained through a homothety are parallel.

Theorem
The set of the middle points of the segments that rest on two give planes is a plane equidistant from the two given planes.

Theorem
The set of points which divide in the same ratio a line which rests on two given planes is a plane parallel to the given planes.

The set of the middle points of the segments that rest on two given lines is a plane parallel to the given plane.

Theorem
The set of points which divide in the same ratio a line, which rests on two given lines is a plane parallel with them.

Dihedral angles

Definition
A dihedral angle is a geometrical figure formed by two semi-planes bounded by the same line.

Elements of a dihedron
a) The edge (the common line of the semi-planes)
b) The faces of the dihedron (the semi-planes)
Two dihedrons are equal if they coincide when super positioned.

Theorem
The corresponding angle plane of a dihedron is the angle formed by the perpendiculars constructed on the two faces on the edge in the same point.

Theorem
Two equal dihedrons have equal plane angles.

Converse

If two dihedrons have equal plane angles, then these are equal.

Perpendicular planes

Definition
Two planes are perpendicular if their dihedral angle is right.

Theorem
A plane which contains a perpendicular line on another plan will be perpendicular on it.

Theorem
The dihedron angles with parallel faces are equal or supplementary.

Polyhedral angle

Definition
The polyhedral angle is the angle formed by the intersection of multiple planes.

Theorem
If two planes are perpendicular, then any line contained on one of them and perpendicular on their line of intersection is perpendicular on the other plane.

Converse
If two planes are perpendicular, then the perpendicular line from a point of a plane on the other plane belongs to the first plane.

Theorem
The locus of the perpendiculars constructed through a point on a line, is a plane which is perpendicular on the line in that point.

Theorem
Given two lines, in order that through one of them to pass a perpendicular plane on the other line it is necessary that the two given lines to be perpendicular.

Theorem
A plane perpendicular on two planes, it is perpendicular on their intersection.

Converse
A plane perpendicular on the edge of a dihedron is perpendicular on its faces.

Definition
The distance from a point to a plane is the perpendicular constructed from that point on the plane.

Theorem
Two dihedrons are adjacent if these have the same edge and a common face.

Bisector plane

Definition
The bisector plane of a dihedron is the plane that divides it in two equal dihedrons.

Theorem
All plane angles of a dihedron are equal.

Theorem
If two secant planes are perpendicular on a third plane, then their line of intersection is also perpendicular on this plane.

Theorem
Through a line which is not perpendicular on a plane it can be constructed only one perpendicular plan on the given plane.

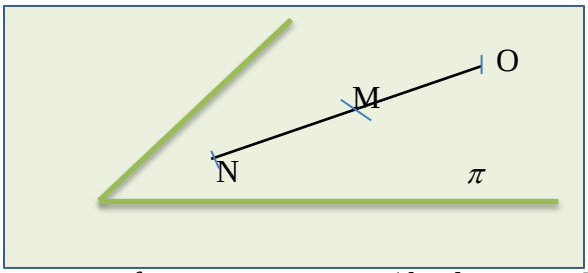
The set of all equidistant points of two planes consists of other two planes perpendicular between them, which are the bisecting planes of the respective dihedron angle.

Theorem
The bisecting planes of a trihedron have a line in common.

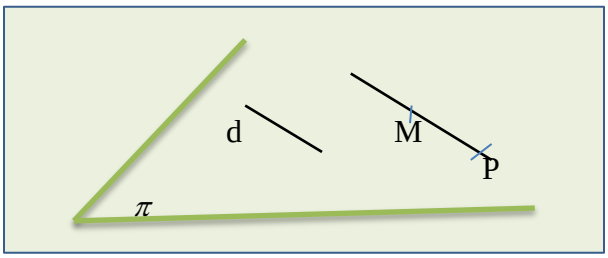
A trihedron has six bisecting planes and four bisectors.

Projections

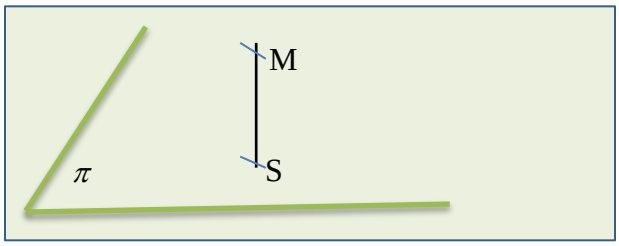
a) Central projection (of center (O), of point M is the intersection of the line ON with the plane π)



b) Projection of a given projection (the direction d is given)



c) Orthogonal projection (we take the intersection of the perpendicular with the plane π - in short we call it projection)



Definition

It is called orthogonal projection of a point A on a plane π the leg of the perpendicular constructed from A on the plane π.

Theorem

The projection of a figure is the locus of the all the projections of all the points of the figure.

The projection on a plane of a line, which is not perpendicular on the plane, is a line.

If the line is perpendicular on the plane, its projection is a point (the point in which it pricks (intersects) the plane).

If the line is parallel to the plane, its projection is equal with the given line.

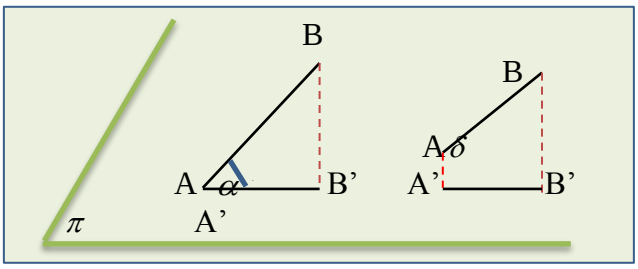
If the line is oblique with respect to the plane, the projected line is smaller in length.

The projection of a geometric figure is also a geometric figure.

The projection in plane of a space figure is a plane geometric figure.

Projected plane δ

The plane from which a line is projected on another plane (these are perpendicular among them)

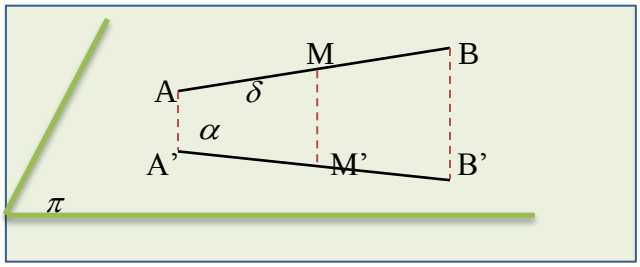


$$A'B' = AB\cos\alpha$$

The projection of a segment is equal to the segment's length multiplied by the cosine of the angle of the line with the plane.

If the projection of a line on a plane is perpendicular on a line from the plane, then the line itself is perpendicular on the line in the plane.

In a projection the ratio of two segments on the same line is the same (maintained).



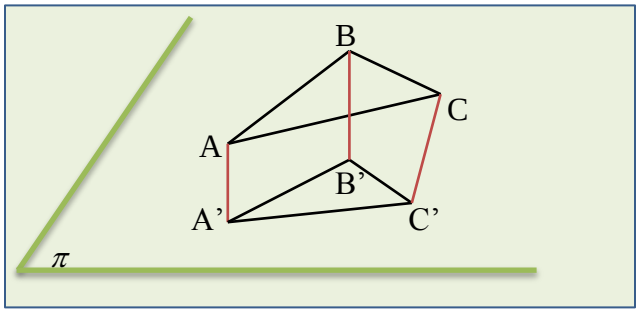
$$\frac{MA}{MB} = \frac{M'A'}{M'B'}$$

Definition

The angle formed by a line with a plane is the angle formed by the line with its projection on the plane.

The angle formed by an oblique line with its projection is the smallest angle formed by it with any other line contained in that plane.

The area of the projection of a triangle on a plane is equal to the area of the triangle multiplied by the cosine of the dihedron angle formed by the triangle's plane with the plane of projection.



$$S' = S\cos\alpha$$

Theorem

A right angle with a side parallel to a plane is projected in this plane by a right angle.

Theorem

An angle which has a side parallel to a plane and its projection with a right angle is a right angle.

The planes which project the edges of a trihedron on the opposite faces have a line in common.

Theorem

If two lines are not coplanar, then there exists only one line which rests on both lines and is perpendicular on both. This line is called common perpendicular of the two lines. It is the smallest distance between two points which belong respectively to the two lines.

If the lines are secant coplanar, their common perpendicular is the perpendicular constructed on their point of intersection on the plane determined by them.

If the lines are parallel, then all perpendicular lines to these lines constructed in their plane, are common perpendicular lines.

Polyhedron

Definition

The polyhedron is a geometric figure formed of many faces (polygons).

There are:

a) Regular polyhedron (its faces are regular equal polygons and its dihedron angles are equal)
b) Non-regular

There are five types of regular polyhedrons:

1) Tetrahedron –solid with four faces (triangles)
2) Hexahedron – solid with six faces (squares)
3) Octahedron - solid with eight faces (triangles)
4) Dodecagon – solid with 12 faces (pentagons)
5) Icosahedron – solid with 20 faces (triangles)

Theorem

Two polyhedrons are equal if by overlapping coincide.

Theorem

The faces of a convex polyhedron are convex polygons.

A line intersects a convex polyhedron at most in two points (if it is not contained on a face).

Definition

A prism is a polyhedron bounded by two bases, equal polygons situated in parallel planes, and by the parallel faces whose number is equal to the number of the sides of the base.

Definition

The prismatic surface is the set of all parallel lines with a given line, and which pass through a closed polygonal line.

Definition

The closed polygonal line is the directional line of the prismatic surface.

Definition

The parallel lines constructed to the given line through the points of the directional line are called the generators of the prismatic surface.

Definition

The generator lines which contain the vertexes of the directional line are called the edges of the prism.

Definition

The intersection of a prismatic surface with n faces with plane which is not parallel to the generators is a polygonal line with n sides.

The classification of prisms

a) The name of the polygon at the base:
   - Triangular
   - Quadrilateral; Example: the parallelepiped whose faces are all parallelograms (random, rectangular)
   - Pentagonal
   - Hexagonal
   - Etc.
   - The polygon with n sides

b) The position of the lateral edges with respect to the base plans
   - Right (the lateral edges are perpendicular on the base plan), the lateral faces are rectangles.
   - Oblique (the lateral edges are oblique with respect to the base plan)

The rectangular parallelepiped is the prism whose base is a rectangle (therefore all faces are rectangles)

The cube is a right prism with three equal concurrent edges in the same vertex. All the faces of a cube are squares.

Definition

The prism height is the perpendicular constructed from a plan to another.

Definition

The prism diagonal is the line segment which connects two vertices which don't belong to a lateral face of the prism.

Definition

The prism's section is the surface obtained by intersecting the prism with a plane.

The section parallel to the prism's base is a polygon equal to the base.

Two parallel planes which section a prismatic surface determine two equal polygons.

Definition

The interior points with respect to a close line P are the points from which any semi line intersects this line.

Definition

The exterior points with respect to a close line P are the points from which it can be constructed semi lines which intersect this line.

Parallelepiped

The parallelepiped is a prism with the base a parallelogram.

Definition

The right parallelepiped is the prism with the base a rectangle.

Properties

1) The four diagonals of a right parallelepiped are concurrent in a point, which is the middle point of each of them, and which is called the symmetry center.
2) The diagonal planes pass also through the symmetry center.
3) The parallelepiped diagonals are equal: $d^2 = a^2 + b^2 + c^2$, in particular for the cubic prism: $d = a\sqrt{3}$.
4) The lateral area of a right prism $A_l =$ The base perimeter x height; the total area $A_t = A_l +$ the area of the two bases; the volume $V =$ the base area x height = the base area x side.

Definition

A polyhedral surface is formed of the polygons on different plans, and which have common sides.

Observation

Two equal solids have the same volume.

Theorem

If two solids (equal or not equal) have the same volume, then these are equivalent.

A pyramidal surface α is determined by a point V and of a polygonal closed plane line $A_1A_2...A_nA_1$, V does not belong to the plane. The surface is made of the set of all the points of the lines which contain the point V and one point of the line $A_1A_2...A_nA_1$.

The edges of the pyramid are the generator lines which pass through the base vertices.

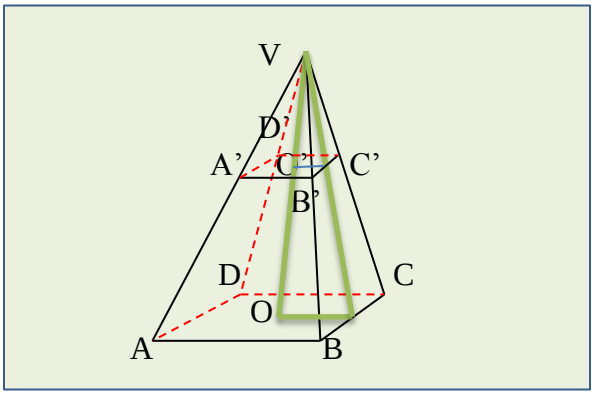
The height is the perpendicular line constructed from the point V on the base plan.

Theorem

A plan which intersects all the edges of a pyramidal surface with n edges intersects the pyramidal surface by a polygonal closed line with n sides.

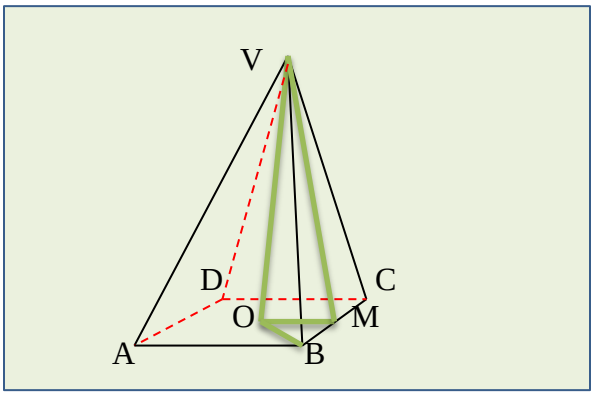
Theorem

The ratio between the section's area and the base's area are equal to the ratio between the squared heights (when the section is parallel to the base).



$$\frac{AriaA'B'C'D'}{AriaABCD} = \frac{VO'^2}{VO^2}$$

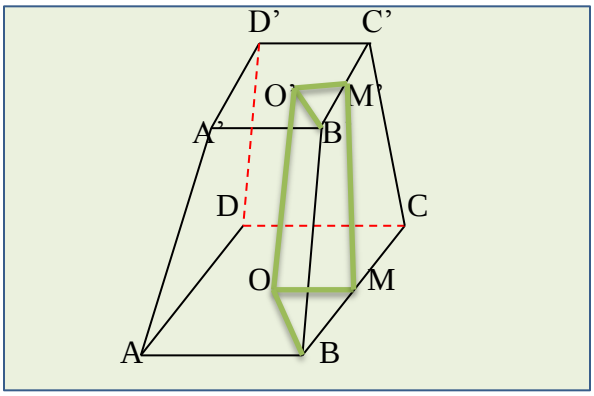
Right triangles which form in a regular pyramid are:



1) ΔVOM (The pyramid height, the base apothem, and apothem of the pyramid).
2) ΔVOB (The pyramid height, the radius of the circumscribed circle to the base, the lateral edge of the pyramid).
3) ΔVMC (The pyramid height, the lateral edge of the pyramid, and half of the base's side).
4) ΔOMC (The base apothem, the circumscribed circle to the base, and half of the base's side).

The section produced by a plane parallel to the base, which intersects one of the lateral edges of the pyramid, is a polygon whose sides are parallel to the sides of the base and which is similar with the base.

Trapezoids which are formed in regular truncated pyramid are:



1) Rectangular trapezoid $OO'M'M$ (the height of the truncated pyramid, the apothems of the bases, apothem of the truncated pyramid).
2) Rectangular trapezoid $OO'B'B$ (the height of the truncated pyramid, the radiuses of the circumscribed circles to the bases, the lateral edge of the truncated pyramid).
3) The isosceles trapezoid $AA'B'B$
4) He isosceles trapezoid $AA'C'C$

The pyramids can be triangular or quadrilateral, etc.

The pyramids can be regular (when the base is a regular polygon and the leg of the height is in the center of the base) or non-regular.

Definition

The median of a tetrahedron is the segment that connects a vertex with the center of mass (barycenter) of the opposite face.

Theorem

The median are concurrent in a point G situated on each of them at the distance of ¾ from the vertex and ¼ from the corresponding face.

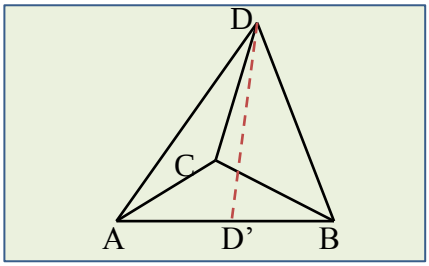
Definition

The median plane of a tetrahedron is the plane which passes through an edge and the middle of the opposite side; these are concurrent in a point G (the point of intersection of the medians).

Definition

The bimedian of a tetrahedron is the segment that connects the middle points of two opposite edges, these are concurrent in a point that is the middle of each of them (G).

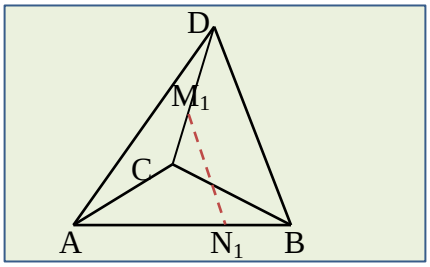
The bisector planes of the dihedrons formed by two adjacent faces of a tetrahedron are concurrent in a point which is the center of the circumscribed sphere to the tetrahedron



DD' median

$$DD'^2 = \frac{1}{3}\left(DA^2 + DB^2 + DC^2\right) - \frac{1}{9}\left(AB^2 + BC^2 + CA^2\right);$$

$\left.\begin{matrix} AA' \\ BB' \\ CC' \end{matrix}\right\}$ *medians;* $AA'^2 + BB'^2 + CC'^2 + DD'^2 = \frac{4}{9}\left(AB^2 + AC^2 + CA^2 + DA^2 + DB^2 + DC^2\right);$



M_1N_1 bimedian

$$M_1N_1^2 = \frac{AD^2 + BD^2 + AC^2 + BC^2 - AB^2 - CD^2}{4};$$

$\left.\begin{matrix} M_2N_2 \\ M_3N_3 \end{matrix}\right\}$ *bimedians;* $M_1N_1^2 + M_2N_2^2 + M_3N_3^2 = \frac{1}{4}\left(AB^2 + AC^2 + CA^2 + DA^2 + DB^2 + DC^2\right) =$

$$= \frac{9}{16}\left(AA'^2 + BB'^2 + CC'^2 + DD'^2\right).$$

An <u>orthogonal tetrahedron</u> is a tetrahedron in which the three pairs of opposed edges are perpendicular: $AB \perp CD;\ BC \perp AD;\ AC \perp BD$.

A <u>spherical sector</u> is the figure generated by the rotation of a circular sector around a diameter which doesn't traverse it.

The locus of the points for which their projections on the sides of a triangle is

a) In plane: the circumscribed circle to the triangle (the Simpson line)
b) In space: the rotation cylinder whose base is the circumscribed circle to the triangle.

Round figures

Definition

A cylindrical surface is the set of the points of all the lines in space constructed through each of the points of line γ, parallel to a given line.

Definition
The line γ is called directing line.

Definition
The parallel lines to the given line constructed through the points of line γ are called the generators of the cylindrical surface.

Classification of the cylinders

a) By the name of the directing line (parabolic, elliptic, circular, etc.)
b) By the angle between the plane of the base with the generator:
   - Right, when the base plane is perpendicular on the generator;
   - Oblique.

Definition
The cylinder circular right is the cylinder which has the base a circle contained in a plane perpendicular on the generator. This results from a complete rotation of a rectangle around an edge.

Definition
The tangent plane to a cylindrical surface is the plane which contains the generator of the cylinder and it is tangent in each point of contact to the circles (curves) of the cylindrical surface.

The generators of the cylinder are equal and parallel, as segments of parallel lines between parallel planes.

Definition
The prism inscribed in a circular cylinder is a prism whose bases are inscribed in the circles of the cylinder bases and having a lateral edge as generator of the cylinder.

All lateral edges of a prism inscribed in a circular cylinder are generators of the cylinder.

In a circular cylinder it can be inscribed a prism with the base a regular polygon with n sides.

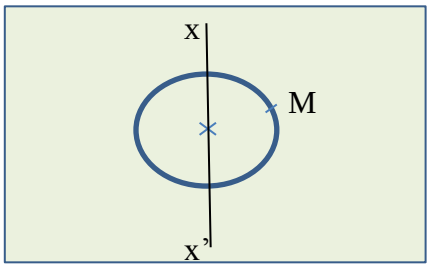
Definition
The prism circumscribed to circular cylinder is the prism whose bases are polygons circumscribed to the base circles of the cylinder, and having a lateral edge parallel to a generator of the cylinder.

The planes which contain the lateral faces of a prism circumscribed to a circular cylinder are tangent to the cylindrical surface.

To any circular cylinder one can circumscribe a prism, which has as bases regular polygons with n sides.

Rotations

Rotation axis xx'



Through the rotation of a figure around an axis, the distances of the points from the axis to the figure will be preserved, and the resulted figures are cold rotational figures.

Through the rotation of a rectangle around one of its sides it is obtained a cylinder circular right.

Through the rotation of a right triangle around one of its cathetus it is obtained a cone circular right.

Through the rotation of a random triangle around one of its sides we obtain two unequal cones, which have the same base.

Through the rotation of an isosceles (or equilateral) triangle around its heath from the vertex of the two equal sides it is obtained a cone.

Through the rotation of a rectangle around the line which connects the middle points of the two opposite sides (the symmetry axis) it is obtained a cylinder.

Through the rotation of an isosceles trapezoid around its symmetry axis, it is obtained a truncated cone.

Any circular cone and right cylinder are called rotational figures.

Definition

Conical surface is the surface which is generated by a line called generator, which moves passing through a fixed point and supports itself on a curve.

The cones are circular (the base is a circle), parabolic, elliptic.

The cones can be right (the height has its leg in the center of the curve), or oblique.

The section performed in a circular cone through a plane parallel to the base which intersects a generator n of the cone, is a circle.

The ratio between the area of the base of a cone circular right and the area of the section performed in the cone through a plane parallel to the base is equal to the square of the ratio between the height of the given cone and the height of the cone formed through section.

In a right circular cone the generators are equal:

$$G^2 = R^2 + I^2$$

Through the section of a right circular cone with a plane parallel to the base it will form a cone that has the radius of the base proportional to the height and the radius of the base of the given cone (and the generator).

Definition

The inscribed pyramid in a circular cone is the pyramid whose base is a polygon inscribed in the circle of the base of the cone and whose vertex coincides with the cone's vertex.

In a cone it can be inscribed a pyramid having as base a regular polygon with n sides.

Definition

The pyramid circumscribed to cone circular is the pyramid, which has as a base a polygon circumscribed to the cone's base circle and its vertex coincides with the cone's vertex.

To any cone it can be circumscribed a pyramid having as base a regular polygon with n sides.

Through a rotation of $180°$ of an isosceles triangle, around a line which contains the base's corresponding height, it will generate a right circular cone.

The truncated cone

$$G^2 = (R - r)^2 + h^2$$

In a truncated cone right circular the generators are equal.

Definition

A truncated circular right cone is the portion of a cone circular right between the base and a parallel section with the base.

Sphere

Definition

A spherical surface is the set of all points from a space, which are at the same distance from a fixed point (a positive number). The fixed point is called the center of the sphere. The diameter of a sphere is the line segment which connects two points on the sphere and passes through the center of the sphere. The chord in a sphere is the line which connects two points on the sphere.

The position of a line with respect to a sphere

a) The line intersects the sphere in two points when $d < R$
b) The line is tangent to the sphere (it has only one common with the sphere) $d = R$.
c) The line is external to the sphere (it does not have any common point with the sphere) $d > R$

The tangent to a sphere is the perpendicular line on the radius on the contact point.

The diameter is the longest chord in a sphere.

The position of a plane with respect to a sphere

a) The secant plane to a sphere (intersects the sphere in a circle) $d < R$
b) The plane is tangent to the sphere (it has a single point in common with the sphere) $d = R$
c) The plane is exterior to the sphere (it does not have any point in common with the sphere)

The plane tangent to a sphere is perpendicular on a radius on its contact point.

Any plane intersects the sphere by a circle.

The largest circle of a sphere is the circle obtained through the section of a sphere with a plane which passes through the center of the sphere; there are an infinite number of such circles.

The sphere is a rotational figure because it results from the rotation of a semicircle around its diameter.

Determination of a sphere

a) The center and the radius
b) The sphere diameter
c) A circle, whose center coincides with the sphere's center (the largest circle of the sphere)
d) Four points, which are not in the same plane) of a sphere.

Definition
The spherical cap is a portion of the sphere's surface limited by a plane which intersects the sphere.

Definition
The cap's base is the circle by which the plane intersects the sphere.

Definition
The cap's height is the distance between the center of the cap's base to the pole of the sphere determined by the diameter which passes through the center of the cap's base.

Definition

The spherical zone is the portion between the sphere's surfaces, limited by two parallel secant planes.

Definition

The zones' bases are the circles by which the two parallel planes intersect the sphere.

Definition

The sphere, as a solid, is formed by the union of all the points of a sphere's surface and of its interior points.

Definition

The spherical sector is the figure obtained through the rotation of a circular sector around a line $n'n$ which contains the center of the circular sector and which does not contain the interior points of the sector.

Definition

The line $n'n$ is called the sector's axis.

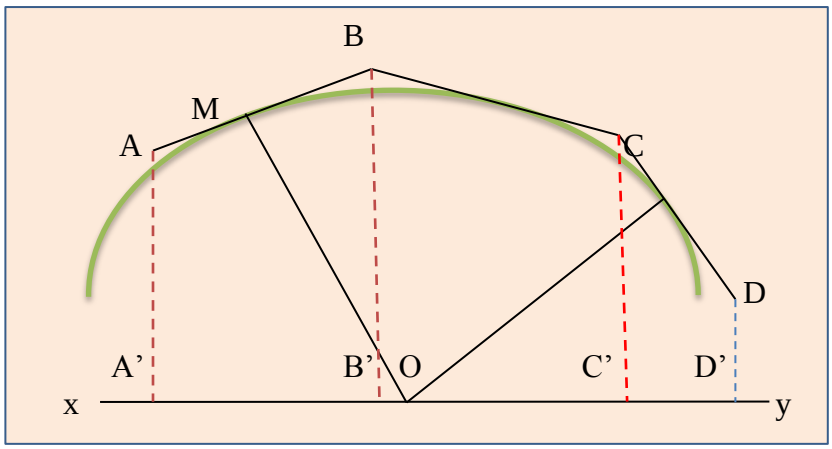
Definition

The radius of the spherical sector is the radius of the circular sector.

Definition

The height of the spherical sector is the distance between the centers of the circles traced by the extremities of the circle of the circular sector.

The area of the surface generated by the rotation of a polygonal regular line around of an axis which contains the center, and which doesn't traverse it, but it is in the same plane with the polygonal regular line, is equal to the projection of the polygonal line on the axis multiplied by the length of the circle whose radius is the apothem of the polygonal regular line.

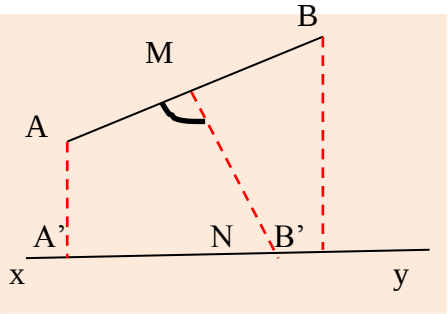


$$S = A'D' \cdot 2\pi \cdot OM$$

The locus of the tangents which can be constructed in a point to a sphere is the tangent plane to the sphere in that point.

The area of the surface generated through the rotation of a segment around of an axis which is in the same plane with the line segment, and which doesn't traverse it, is equal with the segment's projection on the axis multiplied with the length of the circle whose radius is the mediator of the segment whose boundaries are the axis and the segment.

$$S = A'D' \cdot 2\pi \cdot MN$$



Solids inscribed in a sphere

a) Cylinder inscribed in a sphere is the right circular cylinder whose bases are circles of the sphere.
b) Prism inscribed in a sphere is the right prism whose bases are inscribed polygons in the sphere
c) Circular cone inscribed in a sphere is the con whose base is a circle of the sphere and its vertex is on sphere.
d) Pyramid inscribed in a sphere is the prism whose base is a polygon inscribed in a circle of the sphere and its vertex is on the sphere.
e) A truncated cone right circular inscribed in a sphere is the truncated circular cone whose bases are circles of the sphere.
f) A truncated pyramid inscribed in a sphere is the right truncated pyramid whose bases are polygons inscribed in circles of the sphere.

Inscribed spheres

a) Sphere inscribed in a cylinder is the sphere tangent to the bases planes of a cylinder and to the cylinder's generators.
b) Sphere inscribed in a cone is the sphere tangent to the base's plane and to the cone's generators.

Definition

Spherical segment is the part of a sphere contained between two parallel planes which intersect the sphere.

Euclid's theorem

In any polyhedron convex the sum between the number of the faces and the number of the vertexes is bigger by two the number of its edges.

$$F + V = M + 2$$

The areas and the volumes of the most used polyhedrons

1) The right prisms

a) The right prism

$$A_l = P \cdot I$$

$$A_t = A_l + 2 \cdot A_b$$

$$V = A_b \cdot I$$

Where P is the base perimeter; I is the height; A_l is the lateral area; A_t is the total area; A_b is the area of a base; V is the volume

b) The oblique prism

$A_l = P \cdot I$; A_l is the perimeter of the right section multiplied by the edge

$$A_t = A_l + 2 \cdot A_b$$

V = area of the right section multiplied by the edge, therefore equal to the area of the base multiplied by the height.

c) Random parallelepiped

$$A_l = P \cdot I$$

$$A_t = A_l + 2 \cdot A_b$$

$$V = A_b \cdot I$$

d) Rectangular parallelepiped

$A_l = 2(a+b)c$; a,b are the sides of the base, c is the height

$$A_t = 2(ab + bc + ca)$$

$V = abc$; $d^2 = a^2 + b^2 + c^2$

e) Cube

$A_l = 9a^2$; a is the side of the cube

$$A_t = 6a^2$$

$V = a^3$; $d = a^2\sqrt{3}$; d is the diagonal of the cube

2) Regular pyramid

a) Regular pyramid

$A_l = \dfrac{P \cdot A_p}{2}$; A_p is the pyramid apothem

$$A_t = A_l + A_b$$

$$V = \frac{A_b \cdot I}{3}$$

b) Irregular pyramid

$A_l =$ the sum of the areas of the lateral faces.

$$A_t = A_l + A_b$$

$$V = \frac{A_b \cdot I}{3}$$

By sectioning a pyramid with a plane parallel to the base it is obtained a pyramid; the ratio of the volume of the two pyramids is equal to the ratio of their heights cubed:

$$\frac{V'}{V}=\left(\frac{h'}{h}\right)^3$$

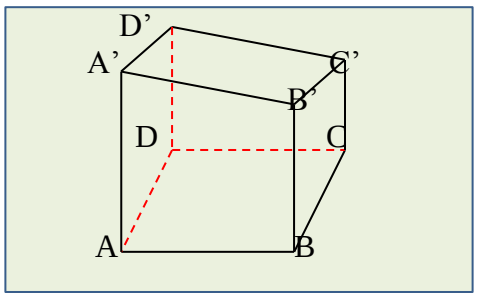
The ratio of the area of the bases is equal to the ratio of their heights squared:

$$\frac{A_b'}{A_b}=\left(\frac{h'}{h}\right)^2$$

Truncated prism is the solid generated through the sectioning of a prism with a plan which is not parallel to the base

$A'B'C'D'$ Parallelogram

$V=$area of the right section multiplied by the arithmetic media of its edges.



c) Truncated pyramid

$A_l = \frac{(P+p)\cdot A_p}{2}$; P is the perimeter of the big base; p is the perimeter of the small base; A_p is the apothem of the truncated pyramid

$A_t = A_l + A_B + A_b$; A_B is the area of the big base; A_b is the area of the small base

$V = \frac{I}{3}\left(A_B + A_b + \sqrt{A_B \cdot A_b}\right)$

The areas and the volumes of the rotation surfaces

1) The circular right cylinder

$A_l = 2\pi RG$

$A_t = 2\pi R(G+R)$

$V = \pi R^2 I$

Where

R = the base radius

G = the generator

I = the height

2) The circular right cone

$A_l = \pi RG$

$A_t = \pi R(G+R)$

$V = \frac{\pi R^2 I}{3}$

3) The truncated circular right cone

$A_l = \pi G(R+r)$

$A_t = \pi G(R+r) + \pi\left(R^2 + r^2\right)$

$V = \frac{\pi I}{3}\left(R^2 + r^2 + Rr\right)$

4) Sphere

a)

$Aria = 4\pi R^2$

$V = \frac{4\pi R^3}{3}$

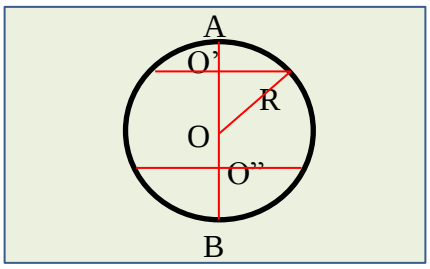
$D = 2R$; $V = A\frac{R}{3}$; D = the sphere's diameter

b)The spherical zone

$Aria = 2\pi RI$

R = the sphere radius

I = the height of the zone $(O'O'')$

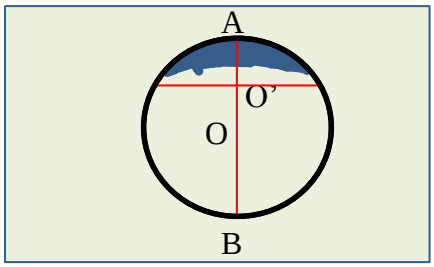


c)The spherical calotte

$$Aria = 2\pi RI$$

R = the sphere radius

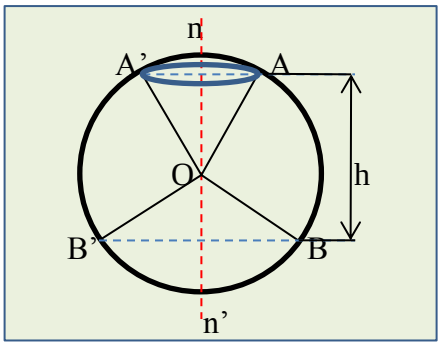
I = the height of the spherical calotte $(O'A)$



d)The spherical sector

$$V = \frac{2\pi R^3 I}{3}$$

R = the sphere radius

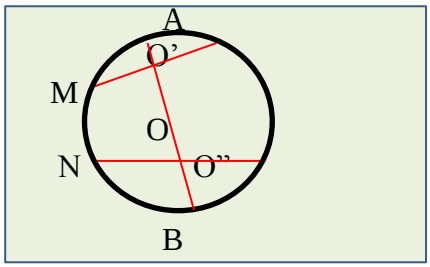


e)The spherical segment

$$V = \frac{4}{3}\pi\left(\frac{h}{2}\right)^3 + \frac{1}{2}\left(\pi r_1^2 h + \pi r_2^2 h\right)$$

r_1, r_2 = the radiuses of the section circles

h = height of the spherical segment (the distance between the planes $(O'O'')$.



When a plane is tangent to the sphere the volume becomes:

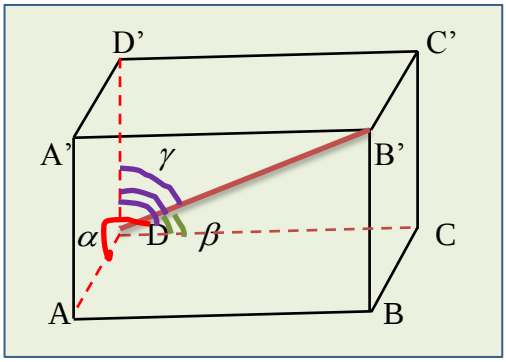
$$V = \frac{\pi h^2}{3}(3R - h)$$

In a pyramid whose edges are equal, the height's leg is in the center of the circumscribed circle of the base polygon.

If in a pyramid the height's leg is in the center of the inscribed circle of the base polygon, then the apothems of the lateral faces are equal (the apothem of the pyramid).

In a right parallelepiped takes place the following relation:

$$\cos^2\alpha + \cos^2\beta + \cos^2\gamma = 1$$



If in a pyramid the vertex is moved parallel to the base, the volume does not change (therefore, it is obtained a pyramid equivalent to the first).

A prismatoid is a polyhedron which has two bases parallel (equal or not equal), eventually, one of them is reduced to a point or a line.

$$V = \frac{h}{6}(Q_1 + Q_2 + 4Q_3)$$

Q_1, Q_2 are the bases areas

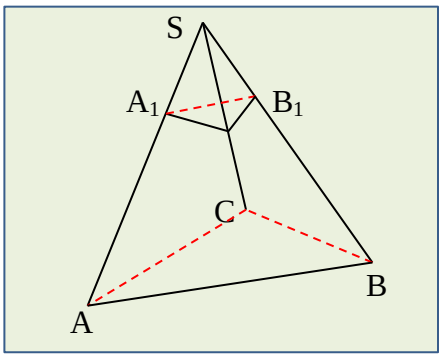
Q_3 is the section's area

The harmonic ratio (bi-ratio) of four points A,B,C,D on a line (taken on this order) is:

$$(ABCD)=\frac{CA}{CB}\div\frac{DA}{DB}$$

In a triangular pyramid given A',B',C' three random points on SA,SB,SC, the following relation takes place (Eugen Rusu).

$$\frac{Vol(SABC)}{Vol(SA'B'C')}=\frac{SA\cdot SB\cdot SC}{SA'\cdot SB'\cdot SC'}$$



The heights of a given tetrahedron denoted h_1,h_2,h_3,h_4 and the distances from an interior point M to the corresponding faces denoted by d_1,d_2,d_3,d_4, the following relation takes place (Eugen Rusu).

$$\frac{d_1}{h_1}=\frac{d_2}{h_2}=\frac{d_3}{h_3}=\frac{d_4}{h_4}=1$$

If in a right pyramid $SABCD$ with the base a rectangle, a random plane cuts the edges in the points $A',B',C'D'$, then

$$\frac{1}{SA'}+\frac{1}{SC'}=\frac{1}{SB'}+\frac{1}{SD'}$$

Chapter Fo□ r:

□ l□ e□ ra

Fro□ □th to □□th

$\pi = 3.141592635...$ is an irrational number

The module of a real number x is the positive value of that number.

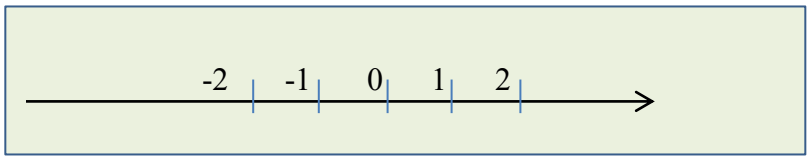
$$|x| = \begin{cases} -x \text{ if } x < 0 \\ 0 \text{ if } x = 0 \\ +x \text{ if } x > 0 \end{cases}$$

$|+3| = 3;$

$|-3| = 3;$

$|0| = 0$

To any real number we can associate a point on the line and only one; If on a line we select a point O called origin and a point which will represent the number 1 (the unity segment), the line is called the real axis or the real line.



Operations with real numbers

Addition

The addition is the operation in which to any pair of real numbers x, y corresponds a real number and only one, denoted $x + y$, and which has:

a) The common sign of x, y, if they have the same sign, and the module is the sum of their modules.
b) The sign of the number whose module is larger and the module is the difference of their modules, in the case that the numbers have different signs.

Multiplication

The multiplication is the operation through which to an pair of real numbers x, y corresponds a real number an if d only one, denoted $x \cdot y$ (xy or $x \times y$), and which has:

a) The sign of $"+"$ if x, y have the same sign, and as module the product of their modules.
b) The sign of $"-"$ if x, y have different signs, and as module the product of their modules.

Algebraic computation

An algebraic expression is a succession of real numbers written with their signs.
Variables are the letters that intervene in an algebraic expression.
Constants are the real numbers (coefficients of the variable).

Example

$E(a,b,c) = 2a^2 + 4b^3 - c$

a, b, c are variables

+2, +4, -1 are constants

$E(a,b,c)$ is an algebraic expression

Algebraic expression:

- Monomial
- Polynomial
  - Binomial
  - Trinomial
  - Etc.

The monomial expression is a succession of signs between which the first is a constant, and the following are different variables separated by the sign of the operation of multiplication.

Examples:

$7x^2 + yz^3; 2x; 4; 0$

Monomial

- The literal part: x^2yz^3 ; x
- The coefficient of the monomial: $7; 4; 0$

The degree of a monomial

a) The degree of a monomial with only one variable is the exponent of the power of that variable.
b) The degree of a monomial which contains multiple variable is the sum of the power of the exponents of the variables.
c) The degree of a monomial in relation to one of its variable is exactly the exponent of the respective variable.

Similar monomials

Similar monomials are those monomials which have the same variables and each variable has the same exponential power.

The sum of several monomials is a similar monomial with the given monomials.

Observation:

If a letter is at the denominator and has a higher exponent than at that from the numerator (example: $4x^2 : 2x^5$) or it is only at the denominator, then we don't obtain a monomial.

Polynomial

A polynomial is a sum of monomials

The numeric value of a polynomial results from the substitution of its variables wit real numbers.

$P(x, y) = 2xy + 3x - 1$

$P(1,0) = 2 \cdot 1 \cdot 0 + 3 \cdot 1 - 1 = 2$

Polynomial of a reduced form

The polynomial of a reduced form is the polynomial which can be represented as a sum of similar monomials.

The degree of a polynomial

The degree of a polynomial in relation to a variable is the highest exponent of the variable.

The degree of a polynomial relative to more variables is equal to the sum of the highest exponents of the variables.

Homogeneous polynomials

The homogeneous polynomials are the polynomials give in a reduced form whose terms are all of the sane degree.

Examples:

$2x; 5x^7; 4x^2 + 3xy - y^2; x + y + z$

To ordinate the terms of a polynomial means to write its terms in a certain order, following certain criteria.

A polynomial with one variable is ordinated by the ascending or descending powers of the variables.

The canonical form of a polynomial $P(x)$ is the ordinate polynomial by the descending powers of x.

The incomplete polynomial is the polynomial which ordinated by the powers of x has some terms of different degrees (smaller than the highest power of x).

Example:

$-2x^6 + 3x^5 + 2$ is an incomplete polynomial (are missing ax^4, bx^3, cx^3, dx)

A polynomial with several variables can be ordinated by the powers of a given variable.

Example:

$P(x,y,z) = -3y^3 + xy^2 + (3x^3 - zx)y + (2x^3 - 2x^2z - 5x^2)$ is ordinated by the powers of y.

The ordination by the homogeneous polynomials

Any given polynomial of a reduced form can be ordinated as a sum of homogeneous polynomials.

Example:

$P(x,y,z) = 2x^3y + 3x + +4y - xy + z^3 - 5 = (2x^3y) + (z^3) + (-xy) + (3x + 4y) + (-5)$

Operations with polynomials

Opposed polynomials are two polynomials whose sum is the null polynomial.

The sum of polynomials

If $P(x) + Q(x) = S(x) \Rightarrow grS(x) \le max[P(x), Q(x)]$

The difference of polynomials

If $P(x)-Q(x)=D(x)\Rightarrow grD(x)\leq max\left[P(x),Q(x)\right]$

The product of polynomials

If $P(x)\cdot Q(x)=D(x)\Rightarrow gr.D(x)=gr.P(x)+gr.Q(x)$

The division of polynomials

- The division without remainder

  If $\frac{P(x)}{Q(x)}=I(x)\Rightarrow gr.I(x)=gr.P(x)-gr.Q(x)$

- The division with reminder

If $\frac{P(x)}{Q(x)}=I(x)$ and $R(x)\Rightarrow gr.I(x)=gr.P(x)-gr.Q(x)$ and $gr.R(x)<I(x)$.

To divide two polynomials of the same variable, we'll ordinate the polynomials by their descending powers of the variable.

A polynomial monomial is a polynomial in which the coefficients of the unknown have a maximum degree of 1.

To divide two polynomials that have several variables, we'll ordinate the polynomials by the powers of a variable and proceed with the division as usual.

Theorem

The remainder of a division of a polynomial $P(x)$ by $x-a$ is equal with the numeric value of the polynomial for which $x-a$, that is $R=P(a)$

Consequence

If $P(x)$ is divisible by $x-a$, then $P(a)=0$.

Formulae used in computations

1) **The product of a sum and difference**

   $(x+y)(x-y)=x^2-y^2$

2) **The square of a binomial**

   $(x+y)^2=x^2+2xy+y^2$

   1. The method of expressing relative to a common factor
   2. The usage of the formulae in computations

      a) $x^2-y^2=(x+y)(x-y)$

      b) $x^3+y^3=(x+y)\left(x^2-xy+y^2\right)$

         $x^3-y^3=(x-y)\left(x^2+xy+y^2\right)$

c) $\left(x^2+2xy+y^2\right)=\left(x+y\right)^2$

$\left(x^2-2xy+y^2\right)=\left(x-y\right)^2$

d) $x^3+3x^2y+3xy^2+y^3=\left(x+y\right)^3$

$x^3-3x^2y+3xy^2-y^3=\left(x-y\right)^3$

e) $x^2+y^2+z^2+2xy+2xz+2yz=\left(x+y+z\right)^2$

f) $x^2+\left(a+b\right)x+ab=\left(x+a\right)\left(x+b\right)$

3. The method of grouping the terms
4. Combined methods

The greatest common divisor (GCD) of several given polynomials is the polynomial with the greatest degree which divides all given polynomials. To determine it we'll take the common irreducible factors at the smallest exponent.

The smallest common multiple of several given polynomials is the polynomial whose degree is the smallest and which is divided by each of the given polynomials. To determine it, we will form the product of the common and non-common irreducible factors at the highest exponent.

Algebraic fractions (algebraic expressions)

An algebraic fraction is an expression of the format $\frac{P}{Q}$, where P,Q are polynomials

To simplify an algebraic fraction is equivalent with writing it into an irreducible format.

To find the common denominator we have to decompose firstly the polynomials denominators in irreducible factors.

Co-prime polynomials are the polynomials which are prime between them.

Algebraic fraction generalized

An algebraic fraction generalized is a fraction of the format:

$$F\left(x,y\right)=\frac{\frac{x+y}{x-1}}{\frac{2x+5}{y+7}}$$

Equalities, equations, system of equations

Definition

An equality is a proposition that refers to the elements of a set M in which the sign "=" appears only one time.

Equality is formed of

- The left side (side I)
- The right side (the side II)

Equality can be:

- True
- False
-

Definition

An equation is the equality which is true only for certain values of the unknown.

To solve an equation means to find the solutions of the give equation.

The equation E_1 implies the equation E_2 only when all the solutions of the equation E_1 are also solutions of the equation E_2 (but not necessarily any solution of E_2 is a solution of E_1).

$P \Leftrightarrow Q \text{ if } P \Rightarrow Q \text{ and } Q \Rightarrow P$

Two equations are equivalent only when have the same solutions.

Properties of an equation in the set of real numbers

Theorem

1) If we add to both sides of an equation (equality) the same element, we'll obtain an equation equivalent to the given equation.
2) If we move a term from a side of equality to the other side and change its sign, we'll obtain an equality equivalent to the given one.
3) If we multiply both sides of equality with a number different of zero, we'll obtain an equality equivalent to the given equality.

The equation of first degree with one unknown

Method of solving it

- If there are parenthesis, we'll open them computing the multiplications or divisions
- If there are denominators we'll eliminate them
- The terms that contain the unknown are separated from the rest, trying to obtain:

  $ax = b \Rightarrow x = \frac{b}{a}$

  This equation has only one solution.

The discussion of the equation of first degree with one unknown

Real parameters are determined real numbers but not effectively obvious

The equation can be:

- Determined (compatible) has a solution
- Not determined: has an infinity od solutions
- Impossible (incompatible) it doesn't have any solution

In a discussion are treated the following cases:

a) The case when the coefficient of x is zero
b) The case when the coefficient of x is different of zero. If the equation contains fractions, a condition that is imposed is that the denominators should be different of zero, otherwise the operations are not defined.

System of equations

Theorems

1) If in a system of equations one equation or several are substituted by one equation or several equations equivalent to those substituted, then we obtain a system of equations equivalent to the initial system of equations.
2) If in a system of equations one equation or several are multiplied by a number different of zero, we'll obtain a system of equations equivalent to the given system of equations.
3) If in a system of equations we substitute one equation by an equation in which the left side contains the sum of the left side members of the equations of the system and in the right side the sum of the right members of the equations, then we will obtain a system of equations equivalent to the given system of equations.

Methods of computation

1) The method of substitution
2) The method of reduction

The systems of equations ca be:

- Determined (compatible) has solutions
- Non-determined – it has an infinity of solutions
- Impossible (incompatible) it does not have solutions

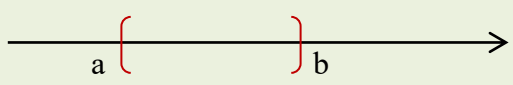
Inequations of first degree

A relation of order is any relation which has the following properties:

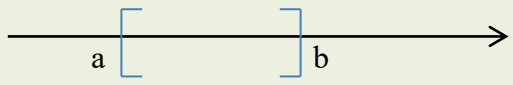
1) $\forall x, y \in \mathbb{R}$, is true at least one of the following propositions: $x > y;\ x = 0;\ x < y$
2) Transitivity
3) Anti-symmetry

Intervals

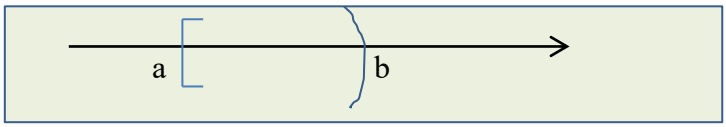
1) Open interval



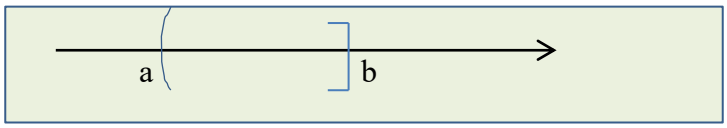
2) Closed interval



3) Interval closed to left and open to the right

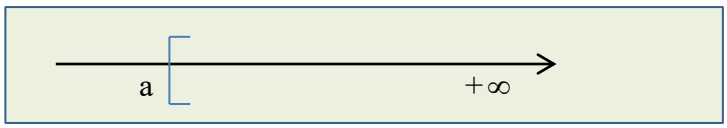


4) Interval open to the left and closed to the right



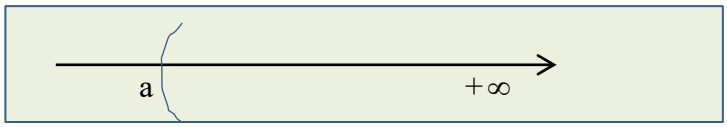
5) Interval closed to the left and unlimited to the right

$[a,+\infty)$



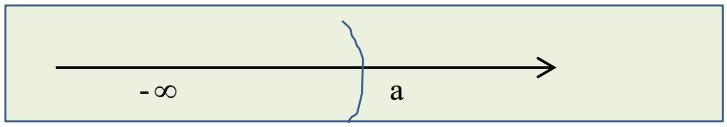
6) Interval open to the left and unlimited to the right

$(a,+\infty)$



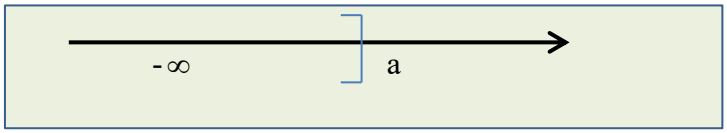
7) Interval open to the right and unlimited to the left

$(-,\infty)$



8) Interval closed to the right and unlimited to the left

$(-\infty,a]$



Properties of the Inequality

1) If the same real number is added to both sides of an inequality, it is obtained an inequality equivalent to the given inequality.
2) If a given inequality is multiplied on both sides by the same real positive number, it will be obtained an inequality equivalent to the given inequality.
   If the inequality is multiplied on both sides with a real negative number then the sense of inequality will change.

Powers with irrational exponent

An irrational algebraic expression is he expression which contains the sign of radical:

$$\sqrt{a^2-3};\sqrt[3]{x+\sqrt{y}};3+\sqrt{\frac{a}{b}}$$

The power of a number is that number multiplied by itself as many times as the power indicates.

$$a^n = a\cdot a\cdot a\cdot \underbrace{.....}_{n\ times}\cdot a$$

a is called the base of the power
n is called the power exponent

- If $x<y\Rightarrow x^n<y^n\ x,y>0;n\in\mathbb{N}$
- If $x=y\Rightarrow x^n=y^n$
- If $x>y\Rightarrow x^n>y^n$
- But, $x^n=y^n \not\Rightarrow x=y$

Radical's definition

Given a positive number A and a natural number $n\geq 2$, a radical of order n of the number A is another positive number, denoted $\sqrt[n]{A}$, which raised at the power of n reproduces the number A.

$$\sqrt[2k]{A^{2k}}=|A|=\begin{cases}A & if\ A\geq 0\\ -A & if\ A<0\end{cases};$$

$$\sqrt{A^2}=\pm A$$

$$\sqrt{(-5)^2}=-(-5)=5;\ \sqrt{(-5)^2}=|-5|=5$$

$$\left(\sqrt[4]{a}\right)^4=a;\ (a\geq 0)$$

Properties of the radicals

1) The amplification of the radical: The value of a radical doesn't change if we multiply by the same natural number the indices of the radical and the exponent of the quantity from inside the radical. $\sqrt[n]{A}=\sqrt[np]{A^p}$
2) The simplification of a radical: The value of a radical doesn't change if we divide by the same number k the indices of the radical and the exponent of the quantity from inside the radical. $\sqrt[np]{A^p}=\sqrt[n]{A}$
   Observation: The simplification of a radical must be done carefully when the indices of the radical is even and there is no precise information about its sign. That's why under the radical we use the module of a quantity: $\sqrt[4]{x^2}=\sqrt[4]{|x|^2}=\sqrt{|x|}$;
   $\sqrt[6]{x^2}=\sqrt[6]{|x|^2}=\sqrt[3]{|x|}$
3) The root of a certain order from a product is equal to the product of the roots of the same order of the factors, with the condition that each factor has a sense. $\sqrt[n]{A\cdot B\cdot ...\cdot V}=\sqrt[n]{A}\cdot\sqrt[n]{B}\cdot ...\sqrt[n]{V};\ (A,B,...,V>0)$
   To make the radicals to have the same index, we'll amplify the radicals getting them to the smallest common multiple.

4) The root of a ratio is equal to the ratio of the roots of the same order of the denominator and numerator, with the condition that both factors are positive. $\sqrt[n]{\frac{A}{B}}=\frac{\sqrt[n]{A}}{\sqrt[n]{B}},\ \frac{\sqrt[n]{A}}{\sqrt[n]{B}}=\sqrt[n]{\frac{A}{B}}$
5) To raise a radical to a power it is sufficient to raise to that power the expression from inside the radical
6) To extract the root from a radical, the roots indexes are multiplied and the expression under the radical remains unchanged. $\sqrt[n]{\sqrt[k]{A}}=\sqrt[nk]{A}$

The extraction of rational factor from a radical

$$\sqrt[n]{a^n b^k}=a\sqrt[n]{b^k}$$

Introduction of a factor under a radical

$$a\sqrt[n]{b}=\sqrt[n]{a^n}\sqrt[n]{b}=\sqrt[n]{a^n b}$$

Elimination of a radical from the denominator

$$\sqrt[m]{\frac{A}{B}}=\frac{\sqrt[m]{A}}{\sqrt[m]{B}}=\frac{\sqrt[m]{A}\cdot\sqrt[m]{B}}{B}=\frac{\sqrt[m]{AB}}{B};\ (A>0,B>0)$$

The reduction of similar radicals

The rationalization of the denominator of a fraction (we amplify with the conjugate)

Conjugate expression of an irrational factor is another expression, which is not identical null, such that their product does not contain radicals

If at the denominator there is an algebraic expression of radicals of the format $\sqrt[3]{a}\pm\sqrt[3]{b}$, we amplify with $\sqrt[3]{a^2}\pm\sqrt[3]{ab}+\sqrt[3]{b}$.

1) $a^m\cdot a^n=a^{m+n};\ (a\neq 0,\ m>n)$
2) $a^m\div a^n=a^{m-n};\ (a\neq 0)$
3) $(a^n)^m=a^{nm};\ (a\neq 0)$
4) $(ab)^n=a^n b^n$
5) $\left(\frac{a}{b}\right)^n=\frac{a^n}{b^n};\ (b\neq 0)$
6) $a^0=1,(a\neq 0)$
7) $a^{-m}=\frac{1}{a^m},(a\neq 0)$

Theorem

If $\frac{p}{m}=\frac{p'}{m'}$, then $a^{\frac{p}{m}}=a^{\frac{p'}{m'}}$

8) $a^{\frac{m}{n}}=a^{\frac{mk}{nk}}=a^{\frac{m\div k}{n\div k}}$

The equation of second degree with one unknown

The general form is $ax^2+bx+c=0;\ (a\neq 0)$

How to find its roots:

$$ax^2+bx+c=0\,|\cdot 4a;\ (a\neq 0)\Rightarrow 4a^2x^2+4abx+4ac=0\Leftrightarrow$$

$$\Leftrightarrow 4a^2x^2+4abx+b^2-b^2+4ac=0\Leftrightarrow (2ax+b)^2-\left(\sqrt{b^2-4ac}\right)^2=0$$

$$\Rightarrow \left(2ax+b+\sqrt{b^2-4ac}\right)\left(2ax+b-\sqrt{b^2-4ac}\right)=0$$

Then the solution will be $x_{1,2}=\dfrac{-b\pm\sqrt{b^2-4ac}}{2a}$

a) In the case in which the coefficient of x is even $b=2b'$ then $x_{1,2}=\dfrac{-b'\pm\sqrt{b'^2-ac}}{a}$

b) In the case in which the coefficient of x is even $b=2b'$ and the coefficient of x^2 is $a=1$, and then $x_{1,2}=-b'\pm\sqrt{b'^2-c}$

Reduced forms of the equation of the second degree

1) In the case $c=0;\ ax^2+bx=0\ \Rightarrow x(ax+b)=0\Rightarrow x_1=0;\ x_2=-\dfrac{b}{a}$

2) In the case $b=0;\ ax^2+c=0\Rightarrow ax^2=-c\Rightarrow x^2=-\dfrac{c}{a}\Rightarrow x_{1,2}=\pm\sqrt{-\dfrac{c}{a}}$

Relations between roots and coefficients

Viète's relation

$$\begin{cases} S=x_1+x_2=-\dfrac{b}{a} \\ P=x_1\cdot x_2=+\dfrac{c}{a} \end{cases}$$

$\Delta=b^2-4ac$:

- If $\Delta<0\Rightarrow$ we have imaginary and conjugated solutions
- If $\Delta=0\Rightarrow$ the solutions are real numbers and equal.
- If $\Delta>0\Rightarrow$ the solutions are real numbers and different.

Irrational equations

Any equation in which the unknown is under the radical constitutes an irrational equation.

To resolve such an equation we'll use the following implication:

$x=y\Rightarrow x^n=y^n$, but $x^n=y^n\not\Rightarrow x=y$.

Precautionary, after determining the solutions of the equation $x^n=y^n$, we need to verify if $x=y$ and eliminate the extra foreign solutions.

We call foreign solutions those solutions which have been introduced through the process of raising to a power.

We must also put the condition that the radical has sense; the solution found must be amongst the values for which the radical makes sense.

If we make successive raising to a power, then we have to put the conditions that both sides are positive.

$$\sqrt[2k]{E(x)} = F(x) \Leftrightarrow \begin{cases} E(x) = \left[F(x)\right]^{2k} \\ E(x) \geq 0 \\ F(x) \geq 0 \end{cases}$$

The set of complex numbers (C)

$z = x + iy;\ i = \sqrt{-1}$

The equality of complex numbers

$z_1 = x_1 + iy_1$

$z_2 = x_2 + iy_2$

$z_1 = z_2$ if $x_1 = x_2$ and $y_1 = y_2$

The addition of complex numbers

$z_1 + z_2 = (x_1 + x_2) + i\ (y_1 + y_2)$

The subtraction of complex numbers

$z_1 - z_2 = (x_1 - x_2) + i\ (y_1 - y_2)$

The multiplication of complex numbers

$z_1 \cdot z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 - x_2 y_1)$

The division of complex numbers

$\frac{z_1}{z_2} = \frac{x_1 + iy_1}{x_2 + iy_2} = \frac{x_1 x_2 + y_1 y_2}{x_2^{\,2} + y_2^{\,2}} + i\frac{-x_1 y_2 + x_2 y_1}{x_2^{\,2} + y_2^{\,2}}$, the amplification with the conjugate

Conjugate complex numbers

$z = x + iy$ and $\overline{z} = x - iy$ with the conditions:

a) $z\overline{z} \in \mathbb{R}$

b) $(z + \overline{z}) \in \mathbb{R}$

Quartic equation

The general form: $ax^4 + bx^2 + c = 0$

Solution: we denote $x^2 = y \Rightarrow x^4 = y^2$

$ay^2 + by + c = 0$

$$y_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \Rightarrow x_{1,2,3,4} = \pm\sqrt{\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}}$$

The following are the conditions that a quartic equation will have all solutions real:

$$\begin{cases}\Delta' = b^2 - 4ac \geq 0\\ S = -\dfrac{b}{a} \geq 0\\ P = +\dfrac{c}{a} \geq 0\end{cases}$$

The reciprocal equation of third degree

A reciprocal equation is the equation whose coefficients at an equal distance from the middle term are equal.

Example:

$$Ax^5 + Bx^4 + Cx^3 + Cx^2 + Bx + A = 0$$

I) $Ax^3 + Bx^2 + Bx + A = 0$

$$A\left(x^3+1\right) + Bx\left(x+1\right) = A\left(x+1\right)\left(x^2 - x + 1\right) + Bx\left(x+1\right) =$$

$$= \left(x+1\right)\left[Ax^2 - \left(A-B\right)x + A\right] = 0$$

$$\Rightarrow \begin{cases} x_1 = -1 \\ x_{2,3} = \dfrac{\left(A-B\right) \pm \sqrt{-3A^2 - 2AB + B^2}}{2A}\end{cases}$$

II) The reciprocal equation of fourth degree

$$Ax^4 + Bx^3 + Cx^2 + Bx + A = 0 \,|\div x^2,\ \left(x \neq 0\right)$$

$$Ax^2 + Bx + C + \frac{B}{x} + \frac{A}{x^2} = 0$$

We'll denote $\left(x + \dfrac{1}{x}\right) = y$, then

$$A\left(y^2 - 2\right) + By + C = 0 \ \Rightarrow Ay^2 + By + \left(-2A + C\right) = 0$$

Systems of equations

The equations of second degree with two unknown

$$\underbrace{ax^2 + bxy + cy^2}_{\substack{terms\ of\ second\\ degree}} + \underbrace{dx + ey}_{\substack{terms\ of\ first\\ degree}} + \underbrace{f}_{\substack{free\\ term}} = 0$$

have an infinity of solutions.

I) This

1) Systems formed of an equation of first degree and an equation of second degree

$$\begin{cases} 2x - 3y = 7 \\ 2x^2 - 3xy + y^2 - 5x + 2y + 4 = 0\end{cases}$$

Is resolved through the substitution method

2) Systems of equations which can be resolved through the reduction method

$$\begin{cases} x^2 - 5xy + y^2 - 3y + 8 = 0 \,|\left(-2\right) \\ 2x^2 - 10xy + 2y + 10 = 0\end{cases}$$

One equation is multiplied by a factor, the equations are added side by side such that one of the unknowns is reduced.

3) Systems of equations in which each equation has on the left side a homogeneous polynomial of second degree and on the right side a constant.

$$\begin{cases} ax^2+bxy+cy^2=d \\ a'x^2+b'xy+c'y^2=d' \end{cases}$$

In particular cases it is applied the reduction method

In general cases it is applied the substitution method

Example

$$\begin{cases} -4x^2-3xy+y^2=-6 \,|\cdot 2 \\ 2x^2-xy-y^2=-4 \,|\cdot(-3) \end{cases}$$

$$\Rightarrow \begin{cases} -8x^2-6xy+2y^2=-12 \\ -6x^2+3xy+3y^2=12 \end{cases} \Rightarrow \begin{cases} -14x^2-3xy+5y^2=0 \,|\div x^2 \\ 2x^2-xy-y^2=-4 \end{cases} \quad (x\neq 0)$$

Homogeneous equations are the equations in which the terms have the same degree.

$$5z^2-3y-14=0;$$

$$z_{1,2}=\frac{3\pm\sqrt{9+280}}{10}=\frac{3\pm 17}{10} \Rightarrow \begin{cases} 2 \\ -\frac{7}{5} \end{cases}$$

The system is reduced to

$$\begin{cases} \frac{y}{x}=2 \\ 2x^2-xy-y^2=-4 \end{cases} \text{ and } \begin{cases} \frac{y}{x}=-\frac{7}{5} \\ 2x^2-xy-y^2=-4 \end{cases}$$

II) Symmetric systems

A symmetric system is a system formed of symmetric equations

An equation is symmetric in x,y if by substituting x by y and y by x, the equation's form does not change.

Examples

$$x+y=a$$
$$4x^2+10xy+4y^2=b$$
$$2x+2y+xy=c$$

Solution

We use the substitution: $x+y=S$, $xy=P$ and we'll find a system which is easier to solve.

If we obtain the solution (a,b), it is obtained also the solution (b,a)

Example

$$\begin{cases} x^2 + y^2 = 5 \\ xy = 2 \end{cases}$$

We denote $x + y = S$ and $xy = P$ then

$$\begin{cases} S^2 - 2P = 5 \\ P = 2 \end{cases} \Rightarrow S^2 - 4 = 5 \Rightarrow S^2 = 9 \Rightarrow S_{1,2} = \pm 3$$

The solutions are: $\begin{cases} S = 3 \\ P = 2 \end{cases}$ and $\begin{cases} S = -3 \\ P = 2 \end{cases}$

Return now to the original unknowns x, y

$$\begin{cases} x + y = 3 \\ xy = 2 \end{cases} \text{ and } \begin{cases} x + y = -3 \\ xy = 2 \end{cases}$$

$$z^2 + 3z + 2 = 0 \Rightarrow z_{1,2} = \frac{3 \pm \sqrt{9-8}}{2} = \frac{3 \pm 1}{2} \text{ with solutions 2 and 1}$$

$$z^2 + 3z + 2 = 0 \Rightarrow z_{1,2} = \begin{cases} -2 \\ -1 \end{cases}$$

The solutions are

$$\begin{cases} x = 2 \\ y = 1 \end{cases} \quad \begin{cases} x = 1 \\ y = 2 \end{cases}$$

$$\begin{cases} x = -2 \\ y = -1 \end{cases} \quad \begin{cases} x = -1 \\ y = -2 \end{cases}$$

III) Other systems are resolved using various operations

- Various substitutions
- Are added or subtract the equations to facilitate certain reductions
- From a system we derive other systems equivalent to the given one

IV) Irrational systems are the systems formed with irrational equations

Methods:

- First we put the conditions that the radicals are positive (if the radical index is even)
- Then the equation is put at the respective power (it is taken into consideration that $A = B \Rightarrow A^n = B^n$, but not vice versa.
- Verify that foreign solutions are not introduced. All the solutions of the initial system are between the solutions of the implied system through raising to the power, but this is not true for the vice versa situation.

Finding the solution for the equation $z^2 = A$ in the set of complex numbers

Let $z = x + iy$, $A = a + bi$

$$z^2 = A \Rightarrow (x + iy)^2 = a + bi$$

$$(x^2 - y^2) + i(2xy) = a + bi$$

We'll use the identification method

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$

which is an equivalent system of equations; then we resolve the system

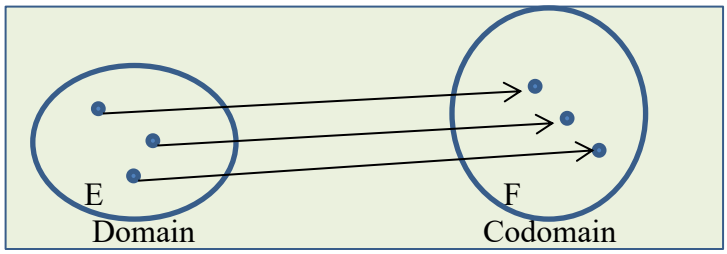
Functions

Given two sets E, F and a relation between the elements of the two sets, such that for any $x \in E$ there exist only one element $y \in F$ in the given relation with x, then we say that it has been defined a function on E with values in F, or an application of the set E in the set F.

- The domain of definition (E) is the set of all the values of x. The arbitrary element x is called the argument of the function
- The set in which the function takes values (F)

$x \to f(x) = y$ (y is the image of x through the function f

$E \xrightarrow{f} F$ or $f : E \to F$



If E or F are finite sets, the function is defined by indicating the correspondence for each element.

$$E = \{a,\ b,\ c,\ d\}$$
$$\downarrow\ \downarrow\ \downarrow\ \downarrow$$
$$F = \{3,\ 1,\ 2,\ 4\}$$

The functions can be:

- Explicit
- Implicit

The function can be classified as:

- Surjective
- Injective (one-to-one function – bijection)
  Bijective

1) Surjective application (or simple surjection) is a function in which the domain coincides with the codomain $f(E) = F$ for $\forall y \in F,\ \exists x \in E : y = f(x)$. Any element from F is the image of an element in E.
2) Injective application or bi-univocal is the function which makes that to pairs of different elements to correspond different values. $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
3) Bijective application (bijection) is the function which is injective and surjective in the same time.

Equal functions

The functions f, g, which have the same argument or different arguments are equal: $f = g$ only the following conditions are satisfied:

a) The functions have the same domain (E)
b) Have values on the same codomain (F)

c) $f(a)=g(a)$

Inverse functions

If $f: E \to F$, the function $f^{-1}: F \to E$ is called the invers function of f.

f^{-1} exists when $f(x)$ is a bijection. Its domain is the set which is a codomain for $f(x)$, and its codomain is the domain for $f(x)$.

Computation of a function inverse

$$f(x)=y=\frac{3x+7}{2};\ f^{-1}(x)=?$$

$$y=\frac{3x+7}{2} \Rightarrow x=\frac{2x-7}{3}$$

$$f^{-1}(x)=\frac{2y-7}{3}$$

The method of complete induction

Induction is defined as the process of going from the particular to general.

If a proposition $P(n)$, where $n \in \mathbb{N}$, satisfies the following conditions:

1) $P(a)$ is true, $(a \in \mathbb{N})$
2) $P(n)=P(n+1)$ for any $n \geq a$, in other words: if we suppose that $P(n)$ is true, it results that $P(n+1)$ is true for any $n \geq a$, then $P(n)$ is true for any natural number $n \geq a$.

The number of subsets of a set with n elements is 2^n

Sums

$$S_1=\sum_1^n k=\frac{n(n+1)}{2}$$

$$S_2=\sum_{k=1}^n k^2=\frac{n(n+1)(2n+1)}{6}$$

$$S_3=\sum_{k=1}^n k^3=\left[\frac{n(n+1)}{2}\right]^2=(S_1)^2$$

$$S_4=\sum_{k=1}^n k^4=\frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$$

To compute $\sum_{k=1}^n k^4$ we start from $(n+1)^5$

$$2^5=(1+1)^5=1^5+5\cdot 1^4+10\cdot 1^3+10\cdot 1^2+5\cdot 1^1+1$$

$$3^5=(2+1)^5=2^5+5\cdot 2^4+10\cdot 2^3+10\cdot 2^2+5\cdot 2^1+1$$

$$4^5=(3+1)^5=3^5+5\cdot3^4+10\cdot3^3+10\cdot3^2+5\cdot3^1+1$$

.....

$$n^5=\left[(n-1)+1\right]^5=(n-1)^5+5\cdot(n-1)^4+10\cdot(n-1)^3+10\cdot(n-1)^2+5(n-1)^1+1$$

$$(n+1)^5=\left[(n)+1\right]^5=n^5+5\cdot n^4+10\cdot n^3+10\cdot n^2+5\cdot n^1+1$$

$$\sum_{k=1}^{n}k^5+(n+1)^5=\sum_{k=1}^{n}k^5+5\sum_{k=1}^{n}k^4+10S_3+10S_2+5S_1+(n+1)$$

$$(n+1)^5=5S_4+10\frac{n^2(n+1)^2}{4}+10\frac{n(n+1)(2n+1)}{6}+5\frac{n(n+1)}{2}+(n+1)$$

$$(n+1)^5=5S_4+\frac{30n^2(n+1)^2+20n(n+1)(2n+1)+30n(n+1)+12(n+1)}{12}$$

Then

$$S_4=\frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$$

Properties of the sums

1) $\sum_{1}^{n}ak=a\sum_{1}^{n}k\,;\ \ a=const$

2) $\sum_{1}^{n}a=na\,;\ a=const$

3) $\sum_{1}^{n}(k)(k+1)=\sum_{1}^{n}(k^2+k)=\sum_{1}^{n}k^2+\sum_{1}^{n}k$

4) $\sum_{k=1}^{n}\frac{A}{k(k+1)}=\sum_{k=1}^{n}\frac{A_1}{k}+\sum_{k=1}^{n}\frac{A_2}{k+1}$

It has been decomposed in simple fractions.

Combinatory analysis

1) Permutation of n elements is the number of bi-univocal applications of a set of n elements on itself.

$P(n)=1\cdot2\cdot3\cdots n=n!$

$n!$ is read "factorial of n.

$(n+1)!=n!(n+1)$

$(n-1)!=\frac{n!}{n}$

$0!=1$, (by definition)

2) Arrangements of n elements taken in groups of m elements ($n\geq m$) is the number of applications bi-univocal of a set of m elements in a set of n elements is

$\underbrace{n(n-1)(n-2)\cdots(n-m+1)}_{m\ factors}$; the elements differ by their nature and their position

$$A_n^m = A_n^{m-1}(n-m+1)$$

3) Combinations of n elements grouped by m elements $n \geq m$ are subsets of m elements formed with elements of a set of n elements

$C_n^m = \frac{A_n^m}{P_m}$; n is called inferior index and m is called superior index.

$$C_n^m = \frac{n!}{m!(n-m)!}$$

Complementary combinations

$$C_n^m = C_n^{n-m}$$
$$C_n^0 = C_n^n = 1$$
$$C_n^1 = C_n^{n-1} = n$$
$$C_n^{m+1} = C_n^m \cdot \frac{n-m}{m+1}$$
$$C_n^{m+1} + C_n^m = C_{n+1}^{m+1}$$

Sums

1) $C_n^1 + C_n^2 + ... + C_n^{n-1} = 2^n - 2$
2) $C_n^0 + C_n^2 + C_n^4 + ... = C_n^1 + C_n^3 + ... = 2^{n-1}$
3) $2^n - C_n^1 2^{n-1} + C_n^2 2^{n-2} - ... + (-1)^n C_n^n = 1$
4) $C_n^0 - C_n^1 + C_n^2 - ... + (-1)^n C_n^n = 0$
5) $C_n^{m+p} + C_p^1 C_n^{m+p-1} + C_p^2 C_n^{m+p-2} + ... + C_n^m = C_{n+p}^{m+p}$

The binomial theorem (Newton)

$$(x+a)^n = C_n^0 x^n a^0 + C_n^1 x^{n-1} a^1 + C_n^2 x^{n-2} a^2 + ... + C_n^k x^{n-k} a^k + ... + C_n^{n-1} x a^{n-1} + C_n^n x^0 a^n$$

The binomial coefficients: $C_n^0,\ C_n^1,\ C_n^2, \ldots, C_n^n$

The general term is: $T_{k+1} = C_n^k x^{n-k} a^k;\ (k = 0,1,...,n)$

The left side of the binomial formula (Newton) is an homogeneous polynomial in relation to x and a (and of n degree).

The binomial coefficients at the extremities or at an equal distance of the two extremities are equal (reciprocal polynomial).

Real functions of real argument

A function of real argument is a function whose domain is the set of real numbers

A real function is that for which the codomain is a set of real numbers.

The graph of a function of real argument $f : E \to F$ is the set of points $M\left(x, f\left(x\right)\right)$

The intersection of the graph with the axes

a) Intersection with axis $Ox : y = 0 \Rightarrow x = a$

b) Intersection with axis $Oy : x = 0 \Rightarrow y = b$

Monotone functions

A real function of real argument $f : E \to F$ is strictly increasing on an interval $I \subset E$, if for any $x_1 \in I$ and $x_2 \in I$ such that $x_1 < x_2$, we have $f\left(x_1\right) < f\left(x_2\right)$

Function of first degree

$$f\left(x\right) = ax + b$$

Any function of first degree is an bi-univocal application of the set of real numbers on the set of real numbers (is a bijective application).

Therefore any function of first degree $f\left(x\right) = ax + b$ has an inverse $f^{-1}\left(x\right) = \frac{1}{a}x - \frac{1}{b}$, and the inverse is a function of first degree.

The function of first degree is strictly monotone on $\mathbb{R}$.

The graphic of a function of the first degree is a line; if $f\left(x\right) = ax; b = 0$ the line passes through the origin, if $f\left(x\right) = ax + b$, the line passes parallel to the line whose equation is $f\left(x\right) = ax$ at the distance b on the axis Oy.

$tag\alpha = a$, α is the angle of the line with the axis Ox.

To construct a line in a Cartesian system we need two points (usually we take the intersections of the line with the axes.

The function of second degree

$$ax^2 + bx + c = a\left(x - x_1\right)\left(x - x_2\right)$$

where x_1, x_2 are the solutions of the equation.

How to write a polynomial of second degree as sum or difference of two squares

$$ax^2 + bx + c = a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2}\right]$$

a) $\Delta > 0$

$$ax^2 + bx + c = a\left[\left(x + \frac{b}{2a}\right)^2 - \left(\frac{\sqrt{\Delta}}{2a}\right)^2\right]$$

b) $\Delta = 0$

$$ax^2 + bx + c = a\left(x + \frac{b}{2a}\right)^2$$

c) $\Delta < 0$

$$ax^2+bx+c=a\left[\left(x+\frac{b}{2a}\right)^2-\left(\frac{\sqrt{-\Delta}}{2a}\right)^2\right]$$

Extremes

1) If $a>0$ $y=ax^2+bx+c$ admits a minimum

$$x_{min}=-\frac{b}{2a}$$

$$y_{min}=\frac{-\Delta}{4a}=\frac{4ac-b^2}{4a}$$

2) If $a<0$, $y=ax^2+bx+c$ admits a maximum

$$x_{max}=-\frac{b}{2a}$$

$$y_{max}=\frac{-\Delta}{4a}=\frac{4ac-b^2}{4a}$$

Intervals of strict monotony

1) If $a>0$, a function of second degree is strictly decreasing on an interval $\left(-\infty,-\frac{b}{2a}\right)$ and is strictly increasing on an interval $\left(-\frac{b}{2a},+\infty\right)$.
2) If $a<0$, the function of second degree is strictly increasing on the interval $\left(-\infty,-\frac{b}{2a}\right)$ and strictly decreasing on the interval $\left(-\frac{b}{2a},+\infty\right)$.

A function $f:R\to R$ is symmetric relative to a line (D) which passes through a point x_0 on the axis Ox and it is parallel to Oy if $f(x_0+h)=f(x_0-h)$ for any $h\neq 0$.

The function of second degree admits as symmetrical axis a line parallel to Oy and passing through the function's point of extreme.

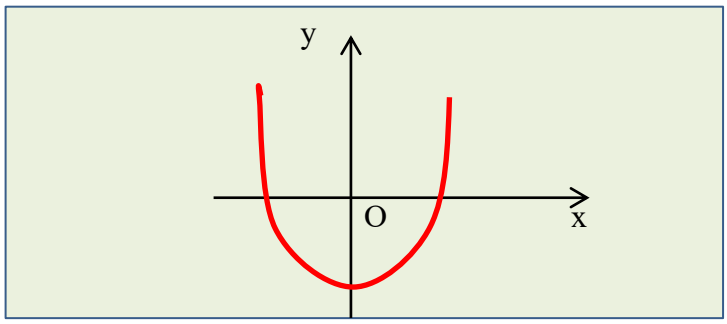
Any value of a function is taken twice: ones in the interval $\left(-\infty,-\frac{b}{2a}\right)$ and the second time on the interval $\left(-\frac{b}{2a},+\infty\right)$, with the exception of the minimum and maximum values which are taken only ones; therefore the function of second degree is not bi-univocal.

The intersection with the axes

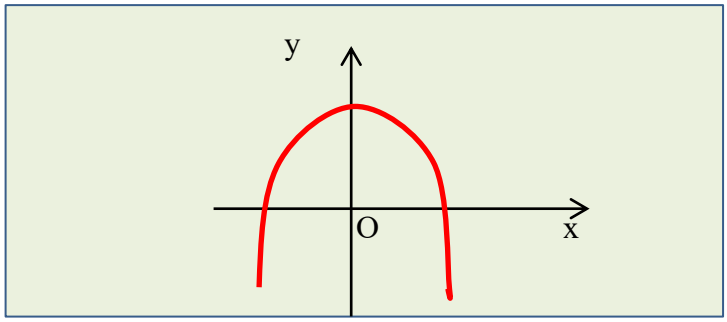
- When $\Delta<0$ then the function does not interest the axis Ox
- When $\Delta=0$ the function intersects the axis $\Delta=0$ in only one point.
- When $\Delta>0$ the function intersects Ox in two distinct points

Graphic – parabola

1) $a > 0$



2) $a < 0$



Parabola is the set of points which are at an equal distance from a fixed point F called focus and from a fixed line (d) called directrix.

$V\left(-\frac{b}{2a}, \frac{-\Delta}{4a}\right)$ the vertex

$F\left(-\frac{b}{2a}, \frac{1-\Delta}{4a}\right)$ the focus

$(d)\, y = \frac{-1-\Delta}{4a}$

The sign of the function of the second degree

a) If $\Delta < 0$, then the function of second degree has the sense of a

b) If $\Delta = 0$, then the function has the sign of a with the exception of the values $x = x_1 = x_2$, where $f(x) = 0$

c) If $\Delta > 0$, then the function has a contrary sense of a between the solutions, and the same sense as a in the exterior of the solutions.

To resolve a system of inequations we intersect the solutions of each inequation.

The nature of the solutions of an equation of second degree with real coefficients which depend of a real parameter

1) $\Delta > 0 \Rightarrow x_1$ and x_2 are real and $x_1 \neq x_2$

2) $\Delta = 0 \Rightarrow x_1 = x_2 \in \mathbb{R}$

3) $\Delta < 0 \Rightarrow x_1 \neq x_2$ are solution imaginary conjugated

The discussion of an equation of second degree with real coefficients dependent of a real parameter

$$S = \frac{b}{a}$$

$$P = \frac{c}{a}$$

$$\Delta = \frac{b^2 - 4ac}{4a}$$

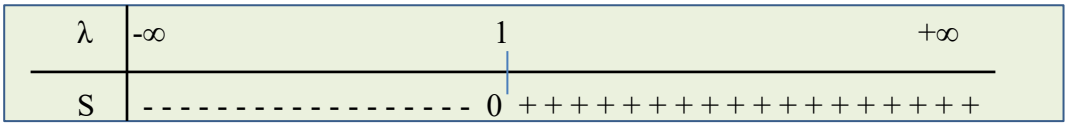
It is studied their signs and are taken all the intervals, as well as the points which delimit the intervals.

Example

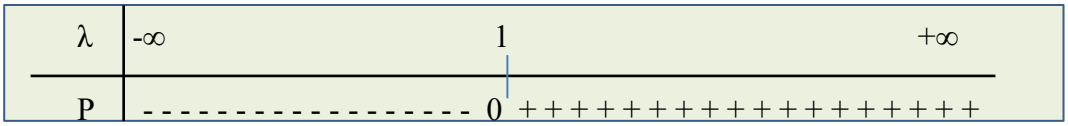
Provide the analysis of the following equation

$x^2 - 2(\lambda - 1)x + 4\lambda - 4 = 0$

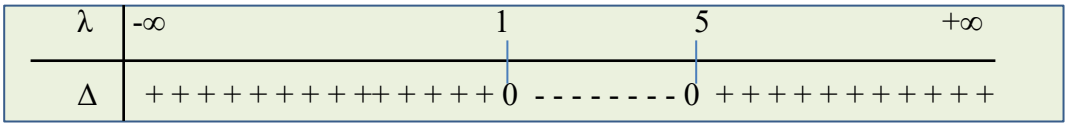
$S = 2(\lambda - 1)$



$P = 4(\lambda - 1)$



$\Delta = \lambda^2 - 2\lambda + 1 - 4\lambda + 4 = \lambda^2 - 6\lambda + 5 = (\lambda - 1)(\lambda - 5)$



Interval	Δ	S	P	Conclusions
$\lambda \in (-\infty, 1)$	+	-	-	The real solutions $x_1 < 0, x_2 > 0; \lvert x_1 \rvert > x_2$
$\lambda = 1$	0	0	0	The real equal solutions $x_1 = x_2 = 0$
$\lambda \in (1,5)$	-	+	+	The imaginary solutions conjugated
$\lambda = 5$	0	+	+	The real equal solutions $x_1 = x_2 = 4$
$\lambda \in (5, +\infty)$	+	+	+	The real different solutions $x_1 > 0, x_2 > 0$

Exponential functions

Properties

1) $f(x_1)\cdot f(x_2)=f(x_1+x_2)$

2) $\dfrac{f(x_1)}{f(x_2)}=f(x_1-x_2)$

3) $\left[f(x_1)\right]^c=f(cx_1)$

4) a) By raising a real number sub unitary (respectively higher than one) to a power with a rational positive exponent we'll obtain a sub unitary number (respectively higher than one)

b)By raising a real number sub unitary (respectively higher than one) to a power with a rational negative we'll obtain a number higher than one (respectively sub unitary).

Exponential function

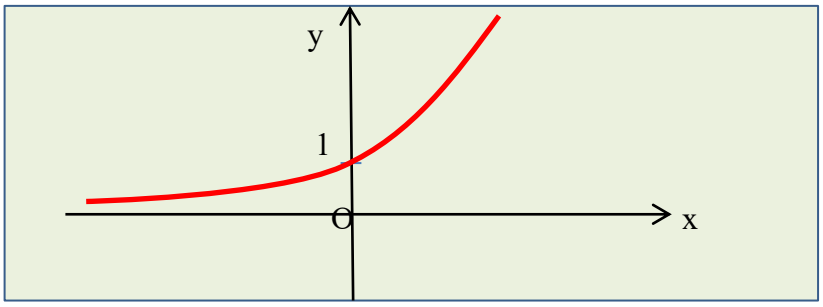
$f(x)=a^x$, where $a>0$ and $a\neq 1$

$f:R\to R_+$

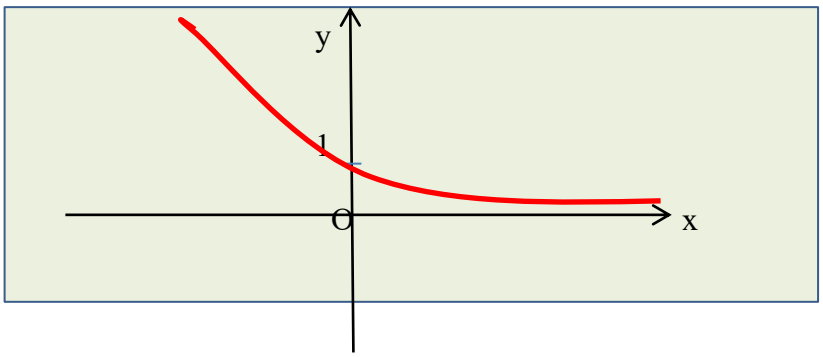
The exponential function is bijective

The monotony

a) If $a>1$ then the function is strictly increasing on the whole domain



b) If $a<1$ then the function is strictly decreasing on the whole domain



Deposits of money to the bank

$f(x)=C\left(\frac{105}{100}\right)^x$

C is the initial amount

x is the number of years

$f(x)$ represents the your sum of money in the bank after an x number of years from the initial deposit.

Exponential equations

1) Equations of the form $a^x=b$, where $b=a^r$; then

   $a^x=a^r\Rightarrow x=r$

   If $b\neq a^r$, then $a^x=b$,

   $x=log_a b$

2) Equations of the form $a^{f(x)}=b$, where $b=a^r$; then

   $a^{f(x)}=a^r\Rightarrow f(x)=r$

   If $b\neq a^r$, we use logarithms

   $a^{f(x)}=b\Rightarrow f(x)=log_a b$

3) Equations of the form $a^{f(x)}=b^{g(x)}$, where $b=a^r$; then

   $a^{f(x)}=a^{rg(x)}\Rightarrow f(x)=r\left(g(x)\right)$

   If $b\neq a^r$, we use logarithms

   $a^{f(x)}=b^{g(x)}\Rightarrow f(x)=\left(log_a b\right)-g(x)$

4) Equations of the form $a^{f(x)}=0$

   We are denote $a^x=y$ and we'll obtain an equation with the unknown y, easy to determine the solutions.

5) Equations which contain the unknown at the base of the powers as well as at the exponent:

   a) The case when the base $x=1$ (we'll verify in the equation)

   b) The case when the base is positive and different of 1.

Logarithms

The logarithm of a number real positive is the exponent of the power to which we must raise the base to obtain that number.

$log_a A=x\Leftrightarrow a^x=A$

The conditions for logarithm's existence

1) $log_a 1=0$

2) $log_a a=1$

3) $log_a a^c = c$

4) $log_a AB = log_a A + log_a B$

5) $log_a \frac{A}{B} = log_a A - log_a B$

6) $log_a A^m = m log_a A$

7) $log_a \sqrt[n]{A} = \frac{1}{n} log_a A$

The collapse (grouping) of an expression containing algorithms

1) $log_a A + log_a B = log_a AB$

2) $log_a A log_a B = log_a \frac{A}{B}$

3) $log_a A = log_a A^c$

4) $k = log_a a^k$

Formulae for changing the base of a logarithm

1) $log_a A = \frac{1}{log_A a} \Rightarrow log_a A log_A a = 1$

2) $log_a A = log_{a^n} A^n$

3) $log_a A = \frac{log_b A}{log_b a}$

$a^{log_a b} = b$

The logarithmic function

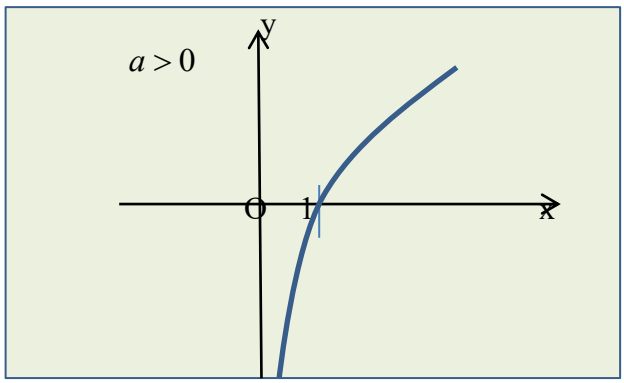
The logarithmic function is the invers of the exponential function (therefore these are symmetric in relation to the first bisector).

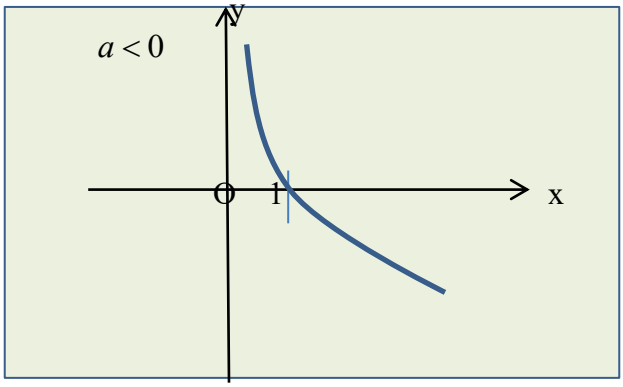
$f(x) = log_a x$

$f : R_+ \to R$

The function is bijective on R_+ if:

- $a > 0$, the function is strictly increasing
- $a < 0$, the function is strictly decreasing





Properties of the logarithmic functions

1) $f(x_1 \cdot x_2) = f(x_1) + f(x_2)$
2) $f\left(\frac{x_1}{x_2}\right) = f(x_1) - f(x_2)$
3) $f(x_1^{\,c}) = cf(x_1)$

The sign of a logarithm

1) $log_a b > 0$ if
   - $a > 1, b > 1$ or
   - $a < 1, b < 1$
2) $log_a b < 0$ if
   - $a > 1, b < 1$
   - $a < 1, b > 1$

Natural logarithms

The natural logarithms are defined as being the logarithms whose base is e=2.71828… (irrational number). The natural logarithms have been introduced by the mathematician Neper, and that's why they are called the neperieni logarithms $ln(A)$

Decimal logarithms

Decimal logarithms are called the logarithms whose base is 10: $lg(A)$. The decimal logarithms have been computed by Brigss. To use them one looks them up in the Mathematical Tables.

The logarithm of a number is formed by:

a) The characteristic, which is the whole part [it is equal to $m-1$, where m represents the number of digits of the given number, eliminating the digits that follow after the decimal point, in the case that the number is above unity].
   - If the number is <1 then its characteristic is negative and equal to the number of zeroes placed in front of the first digit different of zero including also the zero from the whole part. 45.042 = $1+\varepsilon_1$;

     $0.00345 = -3+\varepsilon_2 = \overline{3}+\varepsilon_2$

b) Mantissa (ε):

   $0<\varepsilon<1$

   Mantissa doesn't change if we multiply or divide a number with the powers of 10.

   $$log_{10} A = n+\varepsilon$$

   Sometimes we use the interpolation n method to compute the mantissa.

Operation with logarithms

Addition

$lg\,1534 + lg\,2.23 + lg\,0.022$

$$\begin{array}{r} +3.18583 \\ 0.34830 \\ \overline{2}.34242 \\ \hline 1.87655 \end{array}$$

Subtraction

$lg\,325 - lg\,4116$

$lg\,325 - lg\,4116 = 2.51188 - 3.61448 = 2.51188 - (3+0.61448) =$

$=2.51188-3-1+1-0.61448=\overline{2}.89740$

Cologarithm

The Cologarithm (colog) of a number is equal to the opposite of the logarithm of the given number.

$co\,log\,A = -lg\,A$

$co\,log\,3126 = -lg\,3126 = -(3.49799) = -3-1+1-0.49499 = \overline{4}.50501$

Therefore:

a) To the logarithm's characteristic we add 1 and change the sign of the given number, this way, we obtain the characteristic of the Cologarithm.
b) To obtain the mantissa of the cologarithm we subtract the last digit of the logarithm's mantissa from 10, and the rest of the digits (going to the left direction) from 9.

Multiplication with whole number

a) $8\cdot lg(38.23) = 8\cdot 1.58240 = 12.65920$

b) $5\cdot lg(0.004798) = 5\cdot\overline{3}.68106 = 5\cdot(-3+0.68106) = -15+3.40530 = \overline{12}.40530$

Division with a natural number

a) $\frac{1}{3}lg\,486 = \frac{2.68664}{3} = 0.89554$

b) $lg\sqrt[3]{0.5942} = \frac{\bar{1}.77393}{3} = \frac{-1+0.77393}{3} = \frac{-1-2+2+0.77393}{3} = \bar{1}.92464$

Why are the logarithms as useful?

a) We can transform a product in a sum
b) We can transform a ratio in a difference
c) We can transform a power in a multiplication
d) We can transform a radical extraction in a division

Exponential equations which are resolved using logarithms

1) Exponential equations of the form $a^x = b$

$a^x = b \Rightarrow x = lg_a\, b$ or

$a^x = b \Rightarrow log_{10}\, a^x = log_{10}\, b \Rightarrow x = \frac{lg\, b}{log\, a}$

2) Equations of the form $a^{f(x)} = b$

$a^{f(x)} = b \Rightarrow f(x)\, lg\, a = lg\, b$

$f(x) = \frac{lg\, b}{lg\, a}$

Logarithmic equations

1) Equations of the form $lg_x = A$

$lg_x = A \Rightarrow x = 10^A$

2) Equations of the form $lg\, f(x) = A$

$lg\, f(x) = A \Rightarrow f(x) = 10^A$

3) Equations which contain more logarithms in the same base
   - We group all terms from each side and make an equality from the expressions under the logarithms.
   - To avoid computations with fractions we isolate all terms with the minus sign from the left side in the left side, and the rest in the right side.
   - Other equations are solved through transformations in other bases, and other substitutions.

Exponential and logarithmic systems

For solving these types of systems are used the same procedures as for solving the equations

Conditions imposed for the existence of logarithmic and exponential equations:

a) $log_a b \begin{cases} a > 0 \\ b > 0 \\ a \neq 1 \end{cases}$

b) $a^x \begin{cases} a > 0 \\ a \neq 1 \end{cases}$

Permutations

A permutation is a bi-univocal application from a set A on itself.

Example:

$$\begin{pmatrix} a_1 a_2 a_3 \\ a_3 a_2 a_1 \end{pmatrix}$$

Inversions

An inversion is a per of natural numbers (i_k, i_l) (of a permutation φ) situated in the second line of

$$\begin{pmatrix} 1\ 2\ \ldots\ n \\ i_1 i_2\ \ldots\ i_n \end{pmatrix}$$

with the property $k < l$ and $(i_k > i_l)$

Example

$\begin{pmatrix} 1\ \ 2\ 3 \\ 3\ 2\ 1 \end{pmatrix}$ with the inversions

$(3,1)$ and $(3,2)$.

To determine the number of inversions in φ one counts how many numbers are before first digit (1); then 1 is cut off, one counts how many digits are before 2 (digit one being already excluded); then 2 is cut off, etc. until all digits have been cut off. The sum of all the numbers found before each number cut off.

Any permutation is a product of transpositions.

Permutations can be

- Even – if $Inv(\varphi)$ is an even number
- Odd – if $Inv(\varphi)$ is an odd number

The sign of the permutation

$$\varepsilon(\sigma) = \begin{cases} +1 \ if \ \sigma = even \\ -1 \ if \ \sigma = odd \end{cases}$$

Any permutation has an inverse

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}; \ \ \varepsilon(\sigma \circ \tau) = \varepsilon(\sigma)\varepsilon(\tau)$$

Theorem

If two permutations are obtained one from another through a change of a position, then these are of different classes.

The permutation σ and σ^{-1} have the same sign.

Change of position - Transposition

A transposition is when in a permutation two elements are swapped between them and the rest remained unchanged.

Determinant of order n

A determinant of order n is the number associated to the sum of $n!$ Products of the form $(-1)^{f(\varphi)} a_{1i_1} a_{2i_2} ... a_{ni_n}$

that is:

$$det(A) = \sum_{\psi \in P_n} (-1)^{f(\psi)} a_{j_1 1} a_{j_2 2} ... a_{j_n n}$$

Matrix

A matrix is table of n lines and m columns

$$A = \begin{bmatrix} a_{1,1} a_{1,2} a_{1,3} ... & a_{1,m} \\ a_{2,1} a_{2,2} a_{2,3} ... & a_{2,m} \\ ..... & \\ a_{n,1} a_{n,2} a_{n,3} ... & a_{n,m} \end{bmatrix}$$

The numbers $a_{i,j}$ are called the elements of matrix A

The numbers $a_{j,1}, a_{j,2}, a_{j,3}, ..., a_{j,m}$ form the j line of matrix A

A matrix of type m,n is denoted $A(m,n)$ and it is the matrix with m lines and n columns

A matrix with only one line is

$$A_{1m} = \begin{bmatrix} a_{1,1} a_{1,2} a_{1,3} ... & a_{1,m} \end{bmatrix}$$

A matrix with only one column is

$$A_{n1} = \begin{bmatrix} a_{1,1} \\ a_{2,1} \\ a_{3,1} \\ ... \\ a_{n,1} \end{bmatrix}$$

Square matrix

A square matrix is the matrix that has an equal number of lines as columns

$$A_{nn} = \begin{bmatrix} a_{1,1} a_{1,2} a_{1,3} ... & a_{1,n} \\ a_{2,1} a_{2,2} a_{2,3} ... & a_{2,n} \\ ..... & \\ a_{n,1} a_{n,2} a_{n,3} ... & a_{n,n} \end{bmatrix}$$

Principal diagonal

The principal diagonal is made of elements of the form a_{ii} of a square matrix:

$$a_{11}, a_{22}, ..., a_{nn}$$

The number of even permutations ν_1 and the number of odd permutations ν_2 of a set $\{1,2,...,n\}$ over the same set are in the following relation:

$$\nu_1 = \nu_2 = \frac{1}{2} n!$$

If φ is an identic application $\varphi(h) = h$; $h = 1,2,...,n$, then

$$Inv(\varphi) = 0; \begin{pmatrix} 12...n \\ 12...n \end{pmatrix}$$

The maximum number of inversions is:

$$Inv(\varphi) = \frac{n(n-1)}{2} \begin{pmatrix} 1 & 2 & ... & n \\ n & n-1 & ... & 1 \end{pmatrix}$$

therefore,

$$0 \le Inv(\varphi) \le \frac{n(n-1)}{2}$$

Singular matrix or degenerate

A singular matrix or degenerated is a matrix whose determinant is equal to zero.

Non-degenerate matrix

Anon-degenerate matrix is a matrix whose determinant is different of zero.

A determinant has n lines and n columns

The computation of a determinant of 3X3 matrix –
Sarrus' rule

$$\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix} \begin{matrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \end{matrix}$$

The first two lines are placed under the matrix, then we take with positive (+) sign the products determined by the principal diagonal and others parallel to it, and with negative (-) sign the products of the others.

The rule of triangles

$$\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix}$$

The products that are taken with positive sign form triangles with the side parallel to the principal diagonal

$$\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix}$$

The products that are taken with negative sign form triangles with the side parallel to the other diagonal.

Determinates' properties

The minor of element a_{ij} is a $n-1$ determinant which is obtained by suppressing in a determinant line i and column j $\left(\Delta_{ij}\right)$

The algebraic complement of the element a_{ij} is equal to $(-1)^{i+j}\times$minor of the element: $(-1)^{i+j}\times\Delta_{ij}$.

1) If in a determinant the lines are swapped with the columns, the result is a determinant equal to the given determinant.
2) In in a determinant we swap two lines (or two columns) we obtain a determinant equal in absolute value to the given determinant but of opposite sign.
3) If in a determinant Δ two columns or two lines are equal, then the determinant $\Delta=0$
4) To compute a determinant we use $\Delta=\sum_{i=1}^{n}(-1)^{i+j}a_{ij}\Delta_{ij}$
5) If we multiply a line (or a column) of a determinant with a number, we obtain a determinant equal to the product between the initial determinant and the number.
6) If two lines (or two columns) of a determinant are proportional, then $\Delta=0$
7) If in a determinant a line (or column) has all elements expressed as a sum of two terms, then this determinant can be written as a sum of two determinants in which the rest of the lines remain unchanged, and line k is expressed as a sum of two terms.

$$\begin{vmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \dots & \dots & \dots & \dots \\ a'_{k_1}+a''_{k_1} & a'_{k_2}+a''_{k_2} & \dots & a'_{k_n}+a''_{k_n} \\ \dots & \dots & \dots & \dots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{vmatrix} = \begin{vmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \dots & \dots & \dots & \dots \\ a'_{k_1} & a'_{k_2} & \dots & a'_{k_n} \\ \dots & \dots & \dots & \dots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{vmatrix} + \begin{vmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \dots & \dots & \dots & \dots \\ a''_{k_1} & a''_{k_2} & \dots & a''_{k_n} \\ \dots & \dots & \dots & \dots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{vmatrix}$$

8) If to a line (or a column)of a determinant we add another line (respectively column) multiplied by a number (in particular ±1), we obtain a determinant equal to the given determinant.

If to a line or column we add the sum of the product of other lines with a number (or column) we obtain a determinant equal to the given determinant.

The sum of the product of a line (or column) with numbers is called a linear combination of the respective lines or columns.

The theorem (property) 8 is used to obtain some elements equal to zero on a certain line (or column) which helps to calculate the determinants easily.

Vandermonde determinant of order 3

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix} = (a-b)(b-c)(c-a)$$

This determinant is equal to the product of the differences of these numbers taken in pairs through circular permutations.

Generalization

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ a_1^3 & a_2^3 & \dots & a_n^3 \\ \dots & \dots & \dots & \dots \\ a_1^{n-1} & a_2^{n-1} & \dots & a_n^{n-1} \end{vmatrix} = \text{product of all the different } a_i - a_j;\ 1 \le j < i \le n;$$

$C_n^2 =$ number of factors of the product of differences.

Cramer's rule

This rule is applied to resolve systems of n equations with n unknowns.

If $\Delta \neq 0$, then the system is compatible determined and has unique solution:

$$\left(\frac{\Delta x_1}{\Delta}, \frac{\Delta x_2}{\Delta}, \dots, \frac{\Delta x_n}{\Delta} \right)$$

The Kronecker symbol

$$\delta : E \to \{0,1\}$$

$$\delta((p,q)) = \begin{cases} 1 \ if \ p = q \\ 1 \ if \ p \neq q \end{cases}$$

In a double sum the summation order can be changed

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{ij} = \sum_{j=1}^{m} \sum_{i=1}^{n} \lambda_{ij}$$

Triangular determinant

A triangular determinant is a determinant whose elements above (or under) the principal diagonal are null. This determinant is equal to the product of the elements on the principal diagonal.

$$\begin{vmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ 0 & a_{2,2} & \dots & a_{2,n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{n,n} \end{vmatrix} = a_{1,1} \cdot a_{2,2} \cdot \dots \cdot a_{n,n}$$

Example: Solve the following system using Cramer's rule

$$\begin{cases} 2x + 3y + 4x = 16 \\ 5x - 8y + 2z = 1 \\ 3x - y - 2z = 5 \end{cases}$$

$$\Delta_s = \begin{vmatrix} 2 & 3 & 4 \\ 5 & -8 & 2 \\ 3 & -1 & -2 \end{vmatrix} = 32 + 18 - 20 + 96 + 4 + 30 = 160 \neq 0$$

Therefore, we can apply the Cramer's rule

$$\Delta_x = \begin{vmatrix} 16 & 3 & 4 \\ 1 & -8 & 2 \\ 5 & -1 & -2 \end{vmatrix} = 256 + 30 - 4 + 160 + 32 = 480$$

$$\Delta_y = \begin{vmatrix} 2 & 16 & 4 \\ 5 & 1 & 2 \\ 3 & 5 & -2 \end{vmatrix} = 320$$

$$\Delta_z = \begin{vmatrix} 2 & 3 & 16 \\ 5 & -8 & 1 \\ 3 & -1 & 5 \end{vmatrix} = 160$$

$$x = \frac{\Delta_x}{\Delta_s} = \frac{480}{160} = 3$$

$$y = \frac{\Delta_y}{\Delta_s} = \frac{320}{160} = 2$$

$$z = \frac{\Delta_z}{\Delta_s} = \frac{160}{160} = 1$$

Therefore, the solution is $(3,2,1)$

Δ_{x_n} is obtained by substituting in Δ_s (the system's determinant) the column of the coefficients of x_n with the column of the free (who don't contain unknown) coefficients

Operations with matrices

Addition

The matrices have to be of the same type and we add the corresponding elements.

$$\begin{vmatrix} a'_{1,1} & a'_{1,2} & \dots & a'_{1,n} \\ a'_{2,1} & a'_{2,2} & \dots & a'_{2,n} \\ \dots & \dots & \dots & \dots \\ a'_{m,1} & a'_{m,2} & \dots & a'_{m,n} \end{vmatrix} + \begin{vmatrix} a''_{1,1} & a''_{1,2} & \dots & a''_{1,n} \\ a''_{2,1} & a''_{2,2} & \dots & a''_{2,n} \\ \dots & \dots & \dots & \dots \\ a''_{m,1} & a''_{m,2} & \dots & a''_{m,n} \end{vmatrix} = \begin{vmatrix} a'_{1,1}+a''_{1,1} & a'_{1,2}+a''_{1,2} & \dots & a'_{1,n}+a''_{1,n} \\ a'_{2,1}+a''_{2,1} & a'_{2,2}+a''_{2,2} & \dots & a'_{2,n}+a''_{2,n} \\ \dots & \dots & \dots & \dots \\ a'_{m,1}+a''_{m,1} & a'_{m,2}+a''_{m,2} & \dots & a'_{m,n}+a''_{m,n} \end{vmatrix}$$

Theorem 1

The set $\mathcal{M}_{n,m}$ is a commutative group in relation to the addition in $\mathcal{M}_{n,m}$.

1) $A+(B+C)=(A+B)+C$ associative
2) $A+B=B+A$ commutative
3) $A+\mathcal{O}_{n,m}=A$ neutral element
4) $A+(-A)=\mathcal{O}_{n,m}$ symmetric element
5) The addition is defined

Subtraction

The matrices have to be of the same type and we subtract the corresponding elements.

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{vmatrix} - \begin{vmatrix} a_1' & b_1' & c_1' \\ a_2' & b_2' & c_2' \end{vmatrix} = \begin{vmatrix} a_1 - a_1' & b_1 - b_1' & c_1 - c_1' \\ a_2 - a_2' & b_2 - b_2' & c_2 - c_2' \end{vmatrix}$$

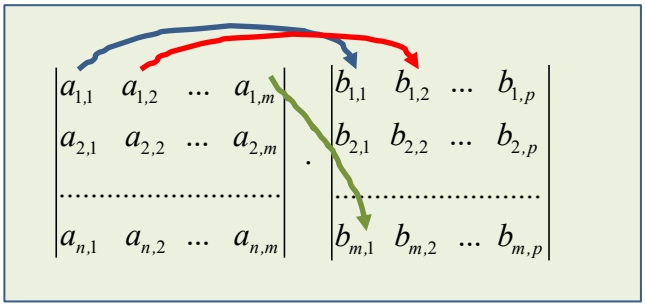
Multiplication

a) Multiplication of a matrix with a number

$$\lambda \begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{vmatrix} = \begin{vmatrix} \lambda a_1 & \lambda b_1 & \lambda c_1 & \lambda d_1 \\ \lambda a_2 & \lambda b_2 & \lambda c_2 & \lambda d_2 \\ \lambda a_3 & \lambda b_3 & \lambda c_3 & \lambda d_3 \end{vmatrix}$$

The number multiplies each elements of the matrix, and we obtain a matrix of the same type.

b) Multiplication of two matrices



To obtain an element $a_{i,j}$ of the product $A_{n,m} \cdot B_{m,p} = C_{n,p}$ we will multiply the line i of the matrix A with the column j of the matrix B (the corresponding element are multiplied and then we perform the sum of the products).

The matrices which can be multiplied cannot be of any type. The condition is:

$A_{n,m} \cdot B_{m,p} = C_{n,p}$

The square matrices can be multiplied between them.

Theorem 2

The set $\mathcal{M}_{n,n}$ is an ring (non-commutative) with unitary element.

1) $\mathcal{M}_{n,n}$ is commutative group in relation to addition
2) The multiplication in $\mathcal{M}_{n,n}$ is associative $A\cdot\left(B\cdot C\right)=\left(A\cdot B\right)\cdot C$
3) The multiplication in $\mathcal{M}_{n,n}$ is distributive at the left and the right in relation with the addition in $\mathcal{M}_{n,n}$

$$\left(A+B\right)C=AC+BC$$

$$A\left(B+C\right)=AB+AC$$

4) The matrix unity U_n is a neutral element in $\mathcal{M}_{n,n}$

$$AU_n=U_nA=A\ \ \left(\forall A\in\mathcal{M}_{n,n}\right)$$

5) $AB\neq BA$ (in general)

The determinant of the product of two square matrices (of the same order) is equal to the product of the determinants of the respective matrices.

$$det\left(AB\right)=det\left(A\right)det\left(B\right)$$

If at least one of the matrices is singular, then the product $A\cdot B$ is singular; if the matrices A,B are non-singular. Then their product is a non-singular matrix.

Transposed matrix

A transpose matrix of another matrix A is the matrix obtained by changing the lines in columns $\left(A^t\right)$

The reciprocal matrix is the matrix obtained by substituting in A^t to each element its algebraic complement $det\left(A^t\right)$, denoted A^*.

A square matrix has an inverse only if it is non-singular.

The invers of a matrix

$$A^{-1}=\frac{1}{det\left(A\right)}A^*$$

$$AA^{-1}=U_n$$

Equations with matrices

1) Multiply with A^{-1} at left

$$X=B\,|\cdot A^{-1}$$

$$A^{-1}AX=A^{-1}B$$

$$U_nX=A^{-1}B$$

$$X=A^{-1}B$$

2) Multiply with A^{-1} at right

$$AX = B \,|\cdot A^{-1}$$

$$AXA^{-1} = BA^{-1}$$

$$XU_n = BA^{-1}$$

$$X = BA^{-1}$$

Resolving a system of equations using matrices

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + a_{1,3}x_3 \ldots \ a_{1,m}x_m = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + a_{2,3}x_3 \ldots \ a_{2,m}x_m = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n,1}x_1 + a_{n,2}x_2 + a_{n,3}x_3 \ldots \ a_{n,m}x_m = b_n \end{cases}$$

$$\begin{Vmatrix} a_{1,1}a_{1,2}a_{1,3}\ldots \ a_{1,m} \\ a_{2,1}a_{2,2}a_{2,3}\ldots \ a_{2,m} \\ \ldots\ldots\ldots\ldots \\ a_{n,1}a_{n,2}a_{n,3}\ldots \ a_{n,m} \end{Vmatrix} \times \begin{Vmatrix} x_1 \\ x_2 \\ . \\ x_m \end{Vmatrix} = \begin{Vmatrix} b_1 \\ b_2 \\ . \\ b_m \end{Vmatrix}$$

The rang of a matrix

Theorem 1

If $A \neq O_{n,m}$ then there is a natural number r unique determined, $1 \leq r \leq min(n,m)$ such that at least one determinant of order r of A is not null, and in the case of $r < min(n,m)$, any determinant of order $r+q$, $q = 1,2,...,min(n,m) - r$ of A is null. (r is the rang of the matrix).

Or

The rang of a matrix is the order of the largest determinant different of zero, which is formed with the elements of A, $r \leq min(n,m)$.

Theorem 2

If all determinants of order p, $p < min(n,m)$ of A are null, then all determinants of order $p+q$ of A, $q = 1,2,...,min(n,m) - p$ are null.

$Pr.\ r(A \cdot B) \leq min\{r(A), r(B)\}$

Systems of n linear equations with m unknown

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + a_{1,3}x_3 \ldots \ a_{1,m}x_m = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + a_{2,3}x_3 \ldots \ a_{2,m}x_m = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n,1}x_1 + a_{n,2}x_2 + a_{n,3}x_3 \ldots \ a_{n,m}x_m = b_n \end{cases}$$

The matrix of the system $S = \|a_{ij}\|$, where: $1 \leq i \leq n,\ 1 \leq j \leq m$.

The rang of the system S rang (S), is the rang of matrix's S.

The complete matrix of the system S is the matrix which is obtained by adding the column of the free terms to matrix of the system.

$$\left\|\begin{array}{l} a_{1,1}a_{1,2}a_{1,3}\ldots\ a_{1,m}b_1 \\ a_{2,1}a_{2,2}a_{2,3}\ldots\ a_{2,m}b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n,1}a_{n,2}a_{n,3}\ldots\ a_{n,m}b_m \end{array}\right\|$$

Determinant principal of a system is the largest determinant different of zero $r \le min(n,m)$ of the system's matrix.

The principal unknown: $x_1, x_2, ..., x_r$

The secondary unknown: $x_{r+1}, x_{r+2}, ..., x_m$

The principal equations are the equations in the principal determinant

The secondary equations are those which are not in the principal determinant.

The determinant obtained by bordering the determinant $\left|\alpha_{ij}\right|$ has an order greater by one than the initial determinant to which we add a line and a column.

The characteristic determinant is obtained by adding to the principal determinant a line and the column of the free terms.

Rouché's theorem

The necessary and sufficient condition that the system S of linear equations (with $r < m$) to be compatible is that all characteristic determinants of the system to be null.

Theorem

The necessary and sufficient condition that all characteristic determinants of a system to be null is that the rank of the system to be equal to the rank of the complete matrix of S.

Kronecker-Cappelli's theorem

The necessary and sufficient condition that the system S to be compatible is that its rang to be equal to the rang of the complete matrix of S.

The necessary and sufficient condition that a system of homogeneous equations to have also other solutions besides the banal one is that the system's rang to be smaller (strictly) than the number of unknowns.

The discussion of a system of n equations with n unknown (non-homogeneous).

1) $n = m$
   a) If $r = n \Rightarrow$ system compatible determined (we'll apply the Cramer's rule)
   b) If $r < n$, we'll apply the Rouché's theorem
      If all $\Delta_{car} = 0 \Rightarrow$ system compatible undetermined
      If at least one $\Delta_{car} \neq 0 \Rightarrow$ system incompatible
2) $n < m$
   a) $r = n \Rightarrow$ system compatible undetermined of the order $m - n$ (apply the Cramer's rule)

b) If $r < n$, we'll apply the Rouché's theorem
Id all $\Delta_{car} = 0 \Rightarrow$ the system is compatible undetermined of the order $m - r$
If at least one $\Delta_{car} \neq 0 \Rightarrow$ the system is incompatible

3) $n > m$
a) If $r = m \Rightarrow$ we'll apply the Rouché's theorem.
b) If $r < m \Rightarrow$ we'll apply the Rouché's theorem

Homogeneous systems

(The free term of each equation is equal to zero)
All homogeneous systems are compatible, having at list the banal solution (0,0,…,0).

1) $n = m$
a) If $r = n \Rightarrow$ The system has only the banal solution
b) $r < n \Rightarrow$ The system is undetermined
2) $n < m$
a) If $r = n \Rightarrow$ The system is undetermined of order $m - n$
b) $r < n \Rightarrow$ The system is undetermined of order $m - r$
3) $n > m$
a) If $r = m \Rightarrow$ The system has only the banal solution
b) If $r < m \Rightarrow$ The is undetermined of order $n - r$.

Problems

1) Show that the equation $2x^4-8x^3+13x^2+mx+n=0$, where $m,n\in\mathbb{R}$, cannot have all the solution real.

$$\begin{aligned}&(x_1-x_2)^2+(x_1-x_3)^2+(x_2-x_3)^2+(x_2-x_4)^2+(x_3-x_4)^2=\\&=3\left(x_1^2+x_2^2+x_3^2+x_4^2\right)-2\left(x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4\right)=\\&=3S_1^2-8S_2=3\cdot4^2-8\cdot\frac{13}{2}=-4<0\end{aligned}$$

Therefore the equation cannot have all the solution real.

2) Show that the equation with real coefficients $2x^4-4x^3+3x^2+ax+b=0$ has all the solution real, then all its solutions are equal.

$$\begin{aligned}&(x_1-x_2)^2+(x_1-x_3)^2+\ldots+(x_3-x_4)^2=\text{ (there are } C_4^2 \text{ parentheses)}\\&=3\left(x_1^2+x_2^2+x_3^2+x_4^2\right)-2\left(x_1x_2+x_1x_3+\ldots+x_3x_4\right)=3S_1^2-8S_2=0\end{aligned}$$

Therefore, $x_1=x_2=x_3=x_4=\frac{2}{4}=\frac{1}{2}$

3) The condition for $E\equiv az^3+bz+c=0$ and $E_1\equiv a'z^3+b'z+c'=0$ to have at least a common solution, we must have

$$aE_1-a'E=\left(ab'-a'b\right)z+\left(ac'-a'c\right)=0$$

The common solution being $z_1=\frac{a'c-ac'}{ab'-a'b}$

4) The primitive solution of an binomial equation (equation with two terms) is the solution which raised to a power 0,1,2,..., $(n-1)$ we'll obtain the n solutions of the given equation.
The primitive solutions are those in which k (from the complex numbers relation) takes prime values with n. The number of the solutions is given by the formula $\varphi(n)$ (Euler's function)

Polynomials

Polynomials with one variable

$$P(x)=2x^4+5x^3-7x+10$$

Polynomials with two variables

$$P(x,y)=x^2+y^2-3xy+x+y-6$$

Polynomials with three variables

$$P(x,y,z)=2x^2+3xyz+x-z+6$$

Definition

A polynomial is a sequence of operations (powers, additions, multiplications) which are computed between the values of the variables (unknowns) and with the coefficients.

The grade of a polynomial in relation to a variable is the exponent of the highest power of the variable:

Example:

$P(z)=a_0z^n+a_1z^{n-1}+...+a_n$ is of grade n, with the essential condition that $a_n\neq 0$; a_0 is called the free term.

The null polynomial

$P^*=0z^n+0z^{n-1}+...+0z+0$

In this case there is no grade.

The grade of the sum of two polynomials

$$Q+P=S$$
$$gr.S\leq max(gr.P,gr.Q)$$

The grade of the difference of two polynomials

$$Q-P=D$$
$$gr.D\leq max(gr.Q,gr.P)$$

The grade of the product of two polynomials

$$A\cdot B=C$$
$$gr.C=gr.A+gr.B$$

The grade of the ratio of two polynomials

$$\frac{M}{N}=A, \text{ and } R$$
$$gr.A=gr.M-gr.N;\ gr.R<gr.N$$

Polynomial function

A polynomial function is a function $P:M\to M$, where M is one of the sets $\mathbb{Z},\mathbb{Q},\mathbb{R}$ or $\mathbb{C}$, such that $P(z)=a_0z^n+a_1z^{n-1}+...+a_n$ and $a_1,a_2,...,a_n\in M$

The difference between a polynomial and a polynomial function is that the polynomial function is characterized by:

- The domain of the definition E
- The set in which the function takes values F
- A rule through which to any element x from E it associates an element unique $P(x)\in F$

The polynomial is characterized only by the third element.

Quantifications

- Universals $\forall$ (for any)
- Existential $\exists$ (exists, at least one)

Identical polynomials

Identical polynomials are two polynomials which define the same function.

Two equal polynomials are identical.

Polynomial identic null

Polynomial identic null is a polynomial which is nullified for any complex value of the variable.

A polynomial $P(z)$ is identical null if, and only if all its coefficients are null $P(z)=P^*$

If a polynomial $P(z)$ of grade n is nullified for $n+1$ values of z then it is identically null.

Two polynomials

$$P(z)=a_0z^n+a_1z^{n-1}+...+a_{n-1}z+a_n$$

$$Q(z)=b_0z^n+b_1z^{n-1}+...+b_{n-1}z+b_n$$

are identical if and only if their corresponding coefficients are equal:

$$a_0=b_0,\ a_1=b_1,...,\ a_n=b_n$$

The method of the undetermined coefficients

$$x^3+2x^2+1\equiv ax^4+bx^3+(b+c)x^2dx+e\Rightarrow\{a=0;b=1;b+c=2\Rightarrow c=1;d=0;e=1\}$$

The division of polynomials

Given two polynomials $D(z),I(z)$, there exists only one polynomial $C(z)$ and only one polynomial $R(z)$ such that we have the identity:

$$D(z)=I(z)\cdot C(z)+R(z)$$

and

$$gr.R(z)<gr.I(z)$$

Using the undetermined coefficients to find the quotient

$$(3z^4-7z^3+12z^2+3z-6)\div(z^2-2z+4)$$

$$3z^4-7z^3+12z^2+3z-6=(z^2-2z+4)(az^2+bz+c)+dz+e$$

$$3z^4-7z^3+12z^2+3z-6=az^4+(-2a+b)z^3+(4a-2b+c)z^2+(4b-2c+d)z+4c+e$$

$$a=3;b=-1;c=-2;d=3;e=2$$

Horner's Rule

$$\left(x^4+3x^2+x-5\right)\div\left(x+2\right)$$

1	0	3	1	-5	
1	-2	7	-13	21	-2

The quotient is

$$x^3-2x^2+7x-13$$

and the remainder 21.

Algebraic equations with complex coefficients

If $P(a)=0$, then the number a is called solution of the equation $P(z)=0$.

The equations can be:

- Algebraic ($x^2-5x=0$)
- Transcendent ($x-2\sin x=0$)

Bezout's theorem

A polynomial $P(z)$ id divided by $z-a$ if, and only if the number a is a solution of the equation $P(z)=0$

A polynomial $A(z)$ is divisible by the polynomial $B(z)$ if there is a polynomial $C(z)$ such that takes place the following equality:

$A(z)=B(z)\cdot C(z)$ for $\forall z,\ z\in C$

Or a polynomial $A(z)$ is divisible by a polynomial $B(z)$ if, and only if the quotient of the division $A(z)\div B(z)$ is the null polynomial

The value of the polynomial $P(z)$ for $z=a$ is the remainder of the division between $P(z)$ and $z-a$. ($P(a)=R$).

If a and b are two solutions of the algebraic equation $P(z)=0$ and $P(z)\div(z-a)=C(z)$, then $C(z)$ is divisible by $(z-b)$

If a polynomial $P(z)$ is divisible by $z-a$ and $z-b$, then it is also divisible by $(z-a)(z-b)$.

The condition for two equations of second degree to have a common solution

$$\begin{cases} ax^2+bx+c=0 \\ a'x^2+b'x+c'=0 \end{cases}$$

$$(ab'-a'b)(bc'-b'c)=(ac'-a'c)^2 \Rightarrow x_1=x_1'$$

x_2 and x_2' arbitrary (these can be equal, or different)

Determining the remainder without performing the division of the polynomials

1) $P(z)\div(z-a)$; the remainder is $P(a)$

2) $P(z)\div(z-a)(z-b)$

$P(z)=Q(z)(z-a)(z-b)+A(z)+B$ (1)

For $z=a$ we substitute in (1) $\Rightarrow P(a)=Aa+B$

For $z=b$ we substitute in (1) $\Rightarrow P(b)=Ab+B$

We obtain the system

$$\begin{cases} P(a)=Aa+B \\ P(b)=Ab+B \end{cases} \qquad (2)$$

The remainder is $A(z)+B$ [A,B determined from system (2)]

3) $P(z)\div(z-a)(z-b)(z-c)$

$P(z)=Q(z)(z-a)(z-b)(z-c)+Az^2+Bz+C$

For $z=a;z=b;z=c$, we obtain

$$\begin{cases} P(a)=Aa^2+Ba+C \\ P(b)=Ab^2+Bb+C \\ P(c)=Ac^2+Bc+C \end{cases} \qquad (3)$$

The remainder is R= Az^2+Bz+C, [A,B,C determined from system (2)]

The fundamental theorem of algebra

Any algebraic equation $P(z)=a_0z^n+a_1z^{n-1}+...+a_{n-1}z+a_n=0$, $a_0,a_1,...,a_n\in C,n\rangle 0$ has at least a solution in C. (Gauss' theorem or d'Alembert's theorem).

The set of the complex numbers is algebraic closed (the enlargement of the notion of number ends when we introduce the complex numbers).

Any polynomial of n degree can be decomposed in n linear, different or equal, factors.

The polynomial decomposition in linear normalized factors is unique.

$$P(z)=a_0(z-z_1)(z-z_2)\cdots(z-z_n)$$

where $z_1,z_2,...,z_n$ are the solutions of the equation $P(z)=0$.

The normalized linear factors are the factors of the form $z-p$ (the coefficient of z must be 1. (Example: $z-\frac{3}{2}$, and not $2z-3$).

An algebraic equation of n degree has n solutions; each multiple solution being counted)

The solutions can be:

- Simple
- Multiple

If in a decomposition of a polynomial in linear factors we have $(z-a)^k$ and this is the highest power of $(z-a)$, we say that a is a multiple solution of order k for the equation $P(z)=0$.

A solution which is not multiple is called a simple solution.

If $P(z)$ has the solutions $z_1, z_2, ..., z_r$ with the orders $k_1, k_2, ..., k_r$ then

$$P(z)=a_0(z-z_1)^{k_1}(z-z_2)^{k_2}\cdots(z-z_n)^{k_r}$$

The condition for two equations of second degree to have a common solution

$$\begin{cases} ax^2+bx+c=0 \\ a'x^2+b'x+c'=0 \end{cases}$$

$$(ab'-a'b)(bc'-b'c)=(ac'-a'c)^2$$

The condition for two equations of n degree to have the same solutions

The condition for two equations of n degree to have the same solutions is that the quotients of the corresponding coefficients to be equal.

$$\frac{a_0}{b_0}=\frac{a_1}{b_1}=...=\frac{a_{n-1}}{b_{n-1}}=\frac{a_n}{b_n}=k$$

Or:

Two algebraic equations have the same solutions with the same order of multiplicity, if, and only if they differ by a constant factor different of zero.

Relations between coefficients and solutions (Viète's relations)

$$P(z)=a_0z^n+a_1z^{n-1}+...+a_{n-1}z+a_n$$

$$S_1=z_1+z_2+...+z_n=-\frac{a_1}{a_0}$$

$$S_2=z_1z_2+z_1z_3+...+z_{n-1}z_n=+\frac{a_2}{a_0}$$

$$S_3 = z_1z_2z_3 + z_1z_2z_4 + ... + z_{n-2}z_{n-1}z_n = -\frac{a_3}{a_0}$$

.....

$$S_k = z_1z_2 \cdots z_k + ... = (-1)^k \frac{a_k}{a_0}$$

.....

$$S_n = z_1z_2 \cdots z_n = (-1)^n \frac{a_n}{a_0}$$

S_1 has C_n^1 terms

S_2 has C_n^2 terms

……..

S_k has C_n^k terms

…….

S_n has C_n^n terms

n is the grade of the polynomial

To resolve an equation it is necessary to have also a relation between the solutions besides those of Viète.

Given a system of $n+1$ equations with n unknown with parameters $a,b,...$, to find the necessary and sufficient condition that the system would be compatible, we select n equations and we solve one of them. Then, we solve the system formed of n with n unknown, and the found values are substituted in the solved equation. The relation obtained between the parameters is the condition that we're looking for.

Multiple solutions

The derivative of a function of a complex variable

$$P(z) = a_0z^n + a_1z^{n-1} + ... + a_n$$

$$a_0, a_1, ..., a_n \in C$$

$$z \in C$$

is the polynomial $P'(z) = na_0z^{n-1} + (n-1)a_1z^{n-1} + ... + a_{n-1}$

A number a is a multiple solution of the order k, $k \in \mathbb{N}$ of the algebraic equation $P(z) = 0$, if, and only if $P(z)$ is divisible by $(z-a)^k$, and the quotient $Q(z)$ is not null for $z = a$; or

A number a is a multiple solution of order k of the equation $P(z) = 0$ if, and only if the polynomial $P(z)$ is divisible by $(z-a)^k$ and is not divisible by $(z-a)^{k+1}$.

Auxiliary proposition

A solution $z=a$ of the algebraic equation $P(z)=0$ is a multiple solution of order k, if, and only if it is a multiple solution of order $k-1$ of the derivative $P'(z)=0$

Theorem

A number is a multiple solution of order k of an algebraic equation $P(z)=0$ if and only it nullifies the polynomial $P(z)$ and the first $k-1$ derivative, and it does not nullify the derivative of the order k.

Complex numbers

$z=a+bi$, $a,b\in\mathbb{R}$, $i=\sqrt{-1}$.

The conjugate of z is $\overline{z}=a-bi$

1) The conjugate of the sum of two complex numbers is the sum of their conjugate: $\overline{z+u}=\overline{z}+\overline{u}$
2) The conjugate of the product of two complex numbers is the product of their conjugate: $\overline{z\cdot u}=\overline{z}\cdot\overline{u}$
3) The natural powers of two imaginary numbers are imaginary conjugate: $\overline{z^n}=(\overline{z})^n$

The values of a polynomial with real coefficients for two imaginary conjugate values of the variable are imaginary conjugated: $P(\overline{z})=\overline{P(z)}$

If an algebraic equation with real coefficients has the solution $u+vi$, then it has also the solution $u-vi$, or:

The imaginary solutions of an algebraic equation with real coefficients are conjugated two by two.

Irrational squared solutions

The numbers of the form $m+n\sqrt{p}$ where $m,n\in\mathbb{Q}$, $p\in\mathbb{N}$ and p does not contain any factor which can be a perfect square.

If an equation with rational coefficients $P(x)=0$ has a solution which is a squared irrational $m+n\sqrt{p}$, then it has also its conjugate $m-n\sqrt{p}$ as solution .

Proposition (SF)

If $m_1\sqrt{p_1}+m_2\sqrt{p_2}$ is a solution on $P(x)$ then $m_1\sqrt{p_1}-m_2\sqrt{p_2}$, $-m_1\sqrt{p_1}+m_2\sqrt{p_2}$, $-m_1\sqrt{p_1}-m_2\sqrt{p_2}$ are solutions for $p\in\mathbb{Q}[x]$. Similarly for three squares.

The transformation in $(-x)$

$P(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$

$P(-x)=a_0(-x)^n+a_1(-x)^{n-1}+\ldots+a_{n-1}(-x)+a_n$

The limits of the solutions

The method of the grouping

The terms are arranged on several groups such that:

a) The coefficient of the first term from each group is positive;
b) Each group has just one variation or none;
c) Research for the smaller integer number, for which each group is positive and this is the superior limit of the solutions.
d) Calculate the transformation in $(-x)$ and find its limit; this will be the inferior limit of the solutions (taken with negative sign $x_i \in (l, L)$

If a polynomial with only one variation $(++++---)$ is positive for a positive value of x greater than a.

If an algebraic equation $P(x)=0$ has the solutions $x_1, x_2, ..., x_n$ its transformation in $-x$ $P(-x)=0$ has the solutions $-x_1, -x_2, ..., -x_n$.

Example

$$P(x)=x^6-3x^5+2x^4+3x^2-31x-96=0$$

$$\left(\underbrace{x^6-3x^5}_{4}\right)+\left(\underbrace{2x^4-31x}_{3}\right)+\left(\underbrace{3x^2-96}_{6}\right)=0 \text{ therefore } L=6$$

$$P(-x)=x^6+3x^5+2x^4+3x^2+31x-96=0$$

$$\left(\underbrace{x^6-96}_{3}\right)+\left(\underbrace{3x^5+2x^4+3x^2+31x}_{1}\right)=0 \qquad \text{therefore } l=-3$$

Then

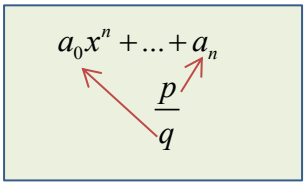
$x_i \in \{-3, 6\}$ where $i=1,2,3,4,5,6$

If an algebraic equation

$$P(x)=a_0x^n+a_1x^{n-1}+...+a_{n-1}x+a_n=0$$

With integer coefficients has as solution the integer p, then a_n is divisible by p.

If an algebraic equation $P(x)=a_0x^n+a_1x^{n-1}+...+a_{n-1}x+a_n=0$ with integer coefficients has as solution the irreducible fraction $\frac{p}{q}$, then a_n is divisible by p and a_0 is divisible by q



The exclusion of some fractions

Let consider the fraction $\frac{a}{b}$:

- If $P(1)$ is not divisible by $b-a$ then the fraction $\frac{a}{b}$ is not a solution

- $P(-1)$ is not divisible by $a+b$ then the fraction $\frac{a}{b}$ is not a solution

Rule

To find the rational solution of an algebraic equation with coefficient integer numbers we'll proceed as follows:

1) Determine the limits L, L' of the solutions
2) Find the integer solutions
3) Determine the fractional solutions (use the Horner' scheme)

A polynomial $P(x)$ is called irreducible in a numeric set ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$) if there exist two polynomials $A(x), B(x)$ with coefficients in that set such that $P(x) = A(x) \cdot B(x)$.

Any polynomial with real coefficients can be decomposed in irreducible factors of I and II degree with real coefficients.

To study the sign of a polynomial we decompose the polynomial in irreducible factors and we study their sign. Then we intersect the signs.

The separation of the solutions through the graphic method

1) The equations of the form $f(x) = 0$
   - Represent the function graphically; the abscises of the points in which the curve intersects the Ox axes are the solutions of the equation
2) Equations of the form $f(x) = g(x)$
   - Both functions are graphically represented; the abscises of the intersection points of the curves are the solutions of the equation.

To limit the interval in which the solutions are located, we give values to the variable and compute, using the Horner's scheme, ($f(a)$ being the remainder); between the contrary signs exits the value zero of the continue function.

The discussion of an equation dependent of a parameter

To discuss an equation we mean to find how many real solutions has the respective equation for different values of a parameter.

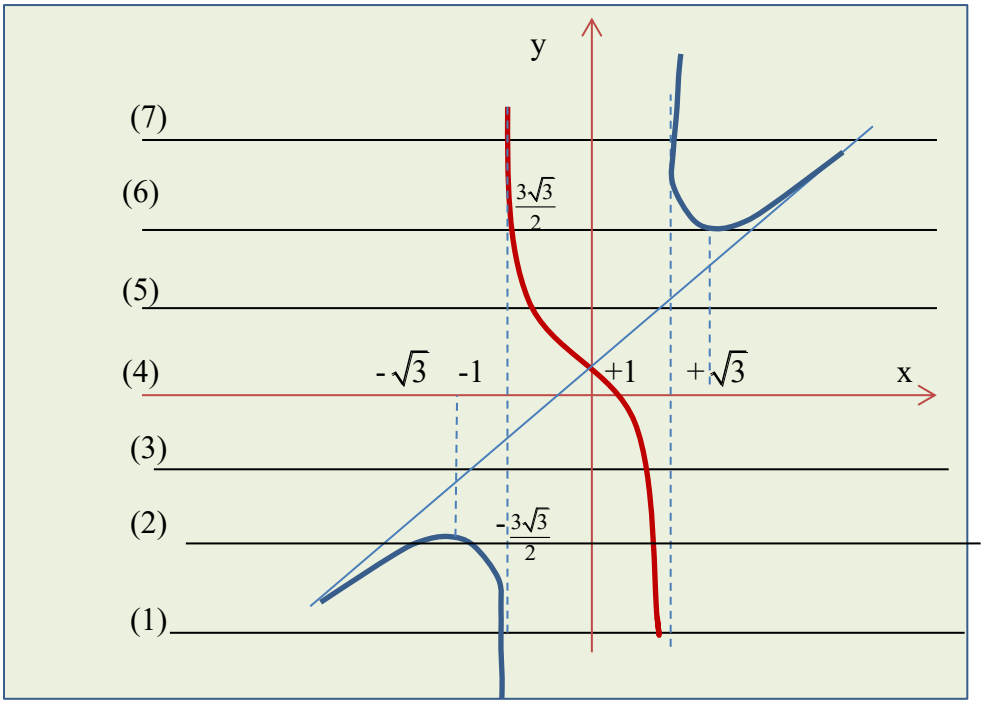
Example

$P(x) = x^3 - ax^2 + a = 0$

$a = \frac{x^3}{x^2 - 1}$

We'll denote $f(x) = \frac{x^3}{x^2 - 1}$ and $g(x) = a$; ($n \in \mathbb{R} \setminus \{-1, +1\}$)

Construct the curves graphs



The table of variation

The values of a	The intervals where the solutions are
$a<-\frac{3\sqrt{3}}{2}$	$\left(-\infty,-\sqrt{3}\right),\left(-\sqrt{3},-1\right),(0,1)$
$a=-\frac{3\sqrt{3}}{2}$	$x_1=x_2=-\sqrt{3}\quad(0,1)$
$-\frac{3\sqrt{3}}{2}<a<0$	$(0,1)$
$a=0$	$x_1=x_2=x_3=0$
$0<a<\frac{3\sqrt{3}}{2}$	$(-1,0)$
$a=\frac{3\sqrt{3}}{2}$	$x_1=x_2=\sqrt{3}\quad(-1,0)$
$a>\frac{3\sqrt{3}}{2}$	$(-1,0),\left(1,\sqrt{3}\right),\left(\sqrt{3},+\infty\right)$

Rolle's theorem

Let f a function defined on an interval $\mathfrak{I}$ and a,b two points in $\mathfrak{I}$ with $a<b$.

If

1) f is continue on the close interval $[a,b]$

2) f is derivable on the open interval (a,b)

3) f has equal values in a,b, $f(a)=f(b)$,

Then there exist at least a point c between a and b, $a<c<b$, in which the derivative becomes null

$f'(c)=0$

Between two consecutive solutions of the equation $f(x)=0$ there exists at least a solution of the equation $f'(x)=0$

Let f a function continue on a closed interval $[x_1,x_2]$, $y_1=f(x_1)$ and $y_2=f(x_2)$ the values of the function at the extremities of the interval and y_3 a number between y_1 and y_2 ($y_1<y_3<y_2$), then there exist at least one point x_3 such that $y_3=f(x_3)$

Or

A continue function does not pass from a value to another value without passing through all intermediary values.

If a function f is continue on a closed interval $[x_1,x_2]$ and $f(x_1)\cdot f(x_2)<0$, then there exists at least a point x_3, $x_1<x_3<x_2$ such that $f(x_3)=0$

Or

A continue function cannot change its sign without becoming zero.

If α,β are two consecutive solutions of the derivative and $f(\alpha),f(\beta)$ are of contrary signs, then between (α,β) there exist only one solution of the equation; if $f(\alpha),f(\beta)$ have the same sign, or $f(\alpha)=0$ or $f(\beta)=0$ the equation does not have in the interval (α,β) any solution.

The equation has at most a solution smaller than the smaller solution of the derivative and at most a solution bigger than the biggest solution of the derivative.

The extremities (left and right) of the interval play the same role as the solutions of the derivative.

The sequence of Rolle

The solutions of the first derivative are written in order, the same the extremities a,b of the interval where the function is defined, and under are written the corresponding values of the function

x	a	x_1	$x_2 \ldots\ldots\ldots x_n$	b
$f(x)$	$\lim\limits_{n\to a} f(x)$	$f(x_1)$	$f(x_2) \ldots\ldots f(x_2)$	$\lim\limits_{n\to\infty} f(x)$

The intervals at the end of which we see values of contrary signs contain a solution of the function $f(\alpha)=0$.

Discussion

Find the intervals in relation to the real parameter of the real solutions of the equation:

$f(x)=3x^4-4x^3-12x^2+a=0$

$f'(x)=12x^3-12x^2-24x+a=0$

$\begin{cases} x_1=1 \\ x_2=0 \\ x_3=2 \end{cases}$

We'll form the Rolle's sequence

x	$-\infty$	-1	0	2	$+\infty$
$f(x)$	$+\infty$	$a-5$	a	$a-32$	$+\infty$
$a<0$	+	-	-	-	+
$a=0$	+	-	0	-	+
$0<a<5$	+	-	+	-	+
$a=5$	+	0	+	-	+
$5<a<32$	+	+	+	-	+
$a=32$	+	+	+	0	+
$a>32$	+	+	+	+	+

We determined the number of the real solutions and the intervals in which these reside.

The approximation of the real solutions of an equation

1) The intervals' separation

   If is known that $x_i \in (a, a+1)$ we can reduce the interval trying the values: $a+0.1; a+0.2; \ldots, a+0.9$

   If $f(a)>0$ and $f(a+1)<0$, and $f(a+0.5)<0$, then $x_i \in (a, a+0.5)$ and so on.

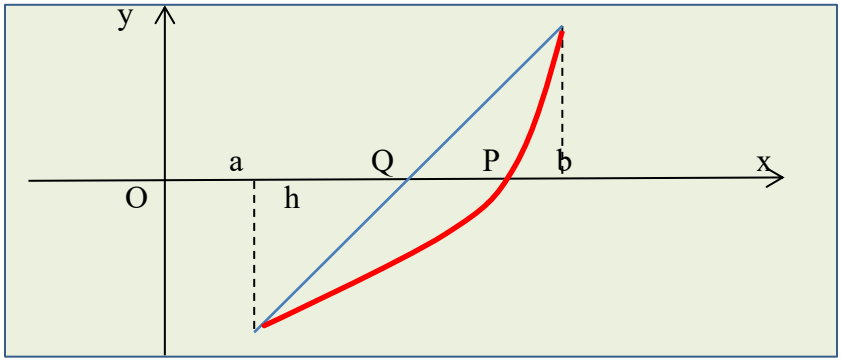
2) The cord method:

   We take the approximate value of the solution the abscise of the point P in which the line MN cuts the axis Ox.

   $MN: y-f(a)=\dfrac{f(b)-f(a)}{b-a}(x-a)$, for $y=0$

$$h = x - a = -\frac{(b-a)f(a)}{f(b)-f(a)}$$

$$x = a + h$$

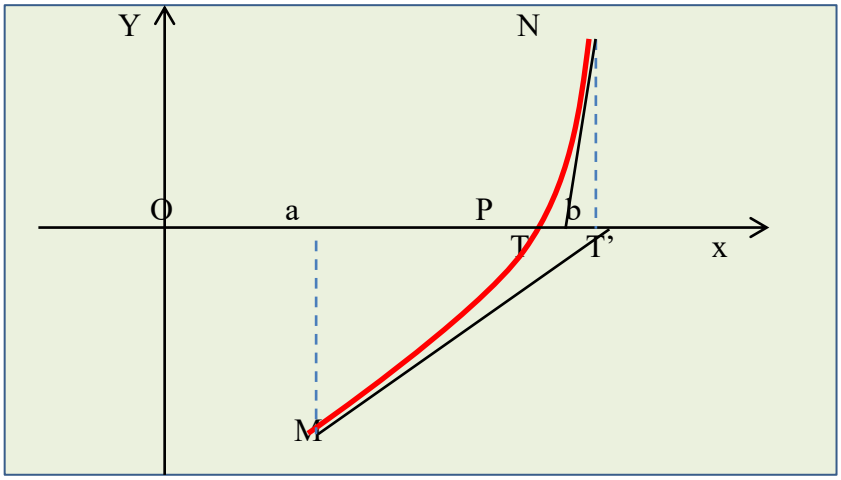


The sense of the error can be determined with the help of a graph or:

1) If $f'(x)\cdot f''(x) > 0$, we have approximation in minus
2) If $f'(x)\cdot f''(x) < 0$, we have approximation in excess

x belonging to the interval in which we computed the solution: (a,b)

3) The method of tangent (Newton's method)



$$MT' : \; y - f(a) = f'(a)(x-a)$$

For $y = 0$

$$h = x - a = \frac{f(a)}{f'(a)}$$

or

$$MT : \; y - f(b) = f'(b)(x-b)$$

For $y = 0$

$$k = x - b = -\frac{f(b)}{f'(b)}$$

- The sense of the error is given by the form of the curve (in minus or in excess)
- The approximations given by the cord method and by the Newton's method are of a contrary sense only when the second derivative maintains its sense in the interval (a,b)
- These methods can be applied repeatedly (to obtain a value more precise)

Laws of internal composition

1) Operations determined with determined elements (numbers) – makes the object of arithmetic
2) Operations determined with determined and undetermined elements – makes the objects of elementary algebra
3) Undetermined operations with undetermined elements makes the object of abstract algebra.

Definition

The law of internal composition between the elements of a set M is an application f defined on a part of the Cartesian product $M \times M$ with values in M (internal algebraic operation).

The corresponding element to a pair (x,y) through the function f is called the composite of x with y $(x \perp y,\ x\mathrm{T}y,\ x \circ y,\ x\Delta y,\ x * y)$

The addition in $\mathbb{C}$ is a function defined on the $\mathbb{C}\times\mathbb{C}$ with values in $\mathbb{C}$. $(f(x,y) = x + y)$ additive.

The subtraction in $\mathbb{C}$ is a function defined on the $\mathbb{C}\times\mathbb{C}$ with values in $\mathbb{C}$. $(f(x,y) = x - y)$.

The multiplication in $\mathbb{C}$ is a function defined on the $\mathbb{C}\times\mathbb{C}$ with values in $\mathbb{C}$. $(f(x,y) = x \cdot y)$

The division in $\mathbb{C}$ is a function defined on the $\mathbb{C}\times\mathbb{C}$ with values in $\mathbb{C}$. $\left(f(x,y) = \frac{x}{y}\right)$

A law of internal composition is defined everywhere if it associates to any pair of elements from M, only one element from M.

Associativity

A law of internal composition which is defined everywhere between the elements of a set E, denoted with the sign T, is called associative if:

$x\mathrm{T}(y\mathrm{T}z) = (x\mathrm{T}y)\mathrm{T}z$ for any elements x,y,z (distinct or not) form E:

$\forall x,y,z \in E : x\mathrm{T}(y+z) = (x\mathrm{T}y)\mathrm{T}z$

Generalized:

$(x_1\mathrm{T}x_2)\mathrm{T}\ldots\mathrm{T}(x_{n-1}\mathrm{T}x_n) = x_1\mathrm{T}x_2\mathrm{T}\ldots\mathrm{T}x_n$ Theorem of associativity

Commutatively

A law of internal composition, everywhere defined, between the elements of set E, denoted $\top$, is commutative if, for any elements x, y from E, we have $x \top y = y \top x$.

$\forall x, y \in E : x \top y = y \top x$

Commutative theorem

$a_1 \top a_2 \top ... \top a_n = a_k \top a_l \top ... \top a_s$, $1 \le k, l, s \le n$

Neutral element

Let E a set on which is given a composition law defined everywhere, denoted $\top$. If there is an element $e \in E$ such that $e \top x = x \top e = x$ for any $x \in E$, this element is called the neutral element for the law $\top$. (The neutral element is unique).

Symmetrical elements

Let E a set for which is defined a composition law denoted $\top$, and for which there exists the neutral element e. An element $x' \in E$ is called the symmetrical of x for the law $\top$, if

$x \top x' = x' \top x = e$

An element p from the set of the remainder's classes modulo m has a symmetrical element in relation to the multiplication, if $(m, p) = 1$ (the two numbers are prime between them). If m is prime, then all elements p have an inverse

If the law is denoted additive, the symmetrical $-x$ is called the opposite of x;

If the law is denoted multiplication, the symmetrical x^{-1} is called the inverse of x; (each element of a set $x \in E$ admits only one symmetric).

Distributive

Let E a set on which are given two internal composition laws $\top$ and $\perp$. We say that the law $\top$ is distributive in relation to the law $\perp$ if for any x, y, z distinct or not from E we have:

$x \top (y \perp z) = (x \top y) \perp (x \top z)$ distributive to the left

$(y \perp z) \top x = (y \top x) \perp (z \top x)$ distributive to the right

Algebraic structure

1) Group
2) Ring
3) Field (a commutative ring)
4) Module
5) Vectorial space
6) Algebra

Group

A composition law forms a group if the following axioms are satisfied

1) The rule is defined everywhere
2) Associativity (A)
3) The existence of the neutral element (N)
4) Any element has a symmetrical (S)

If the law is commutative we called the group abelian (or commutative)

Immediate consequences of the group's axioms

a) The composite of three, four, or more elements is the same (A)
b) In a group exists a neutral element and only one (N)
c) Any element admits a symmetrical and only one (S)
d) In a group G whose law is denoted multiplication we have: $\left(x^{-1}\right)^{-1} = x$

- In a group multiplicative $x \cdot x \cdot x \cdot \cdot x = x^n$ (the nth power of x)
- In a group additive $x + x + x + \cdot\cdot + x = nx$

$$x^n x^m = x^{n+m}$$
$$\left(x^n\right)^m = x^{nm}$$
$$nx + mx = (n+m)x$$
$$m(nx) = (mn)x$$
$$(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$$
$$\left(x^{-1}\right)^n = \left(x^n\right)^{-1} \quad n \in \mathbb{N}$$

Simplification at the left and at the right

$$(a \top x = b \top x) \Rightarrow (a = b)$$
$$(x \top a = x \top b) \Rightarrow (a = b)$$
$$(a = b) \Leftrightarrow (a \top x = b \top x)$$
$$(a = b) \Leftrightarrow (x \top a = x \top b)$$

Equations in a group

1) $a \top x = b$

$$a' \top (a \top x) = a' \top b$$
$$(a' \top a) \top x = a' \top b$$
$$e \top x = a' \top b$$
$$x = a' \top b$$

2) $x \top a = b$

$$(x \top a) \top a' = b \top a'$$
$$x \top (a \top a') = b \top a'$$
$$x \top e = b \top a'$$

$$x = b \top ba'$$

Ring

Two composition rules, first denoted additive and the second multiplicative define on a set a structure ring I if:

1) A_P The addition is defined every where
2) A_A The addition is associative
3) A_C The addition is commutative
4) A_N There exists a neutral element (0)
5) A_S Any element admits a symmetrical
6) M_P The multiplication is defined everywhere
7) M_A The multiplication is associative
8) D_{MA} The multiplication is distributive in relation to addition

If the multiplication is commutative we call the ring commutative
If there is a neutral element in relation to the multiplication, we say that the ring has the unity element

Divisors of zero

An element $d \neq 0$ of a ring is called divisor of zero, if there exists an element $d' \neq 0$ such that $dd' = 0$ or $d'd = 0$.

The rule of signs in a ring

$$(-a)\cdot b = a\cdot(-b) = -(ab)$$
$$(-a)\cdot(-b) = ab$$

The simplification to the left and to the right in ring without divisors of zero

$$ax = ay \Rightarrow x = y \quad (a \neq 0)$$
$$xa = ya \Rightarrow x = y \quad (a \neq 0)$$

Field

Two composition rules, first denoted additive and the second multiplicative, determine on a set a structure of field if

1) A_P The addition is defined every where
1) A_A The addition is associative
2) A_C The addition is commutative
3) A_N There exists a neutral element (0)
4) A_S Any element admits a symmetrical
5) M_P The multiplication is defined everywhere

6) M_A The multiplication is associative

7) M_N There exists a neutral element (0)

8) D_{MA} The multiplication is distributive in relation to addition

9) M_S Any element admits a symmetrical

If the multiplication is commutative then the field is called commutative
In a field there are no divisors of zero.

Wedderburn's theorem

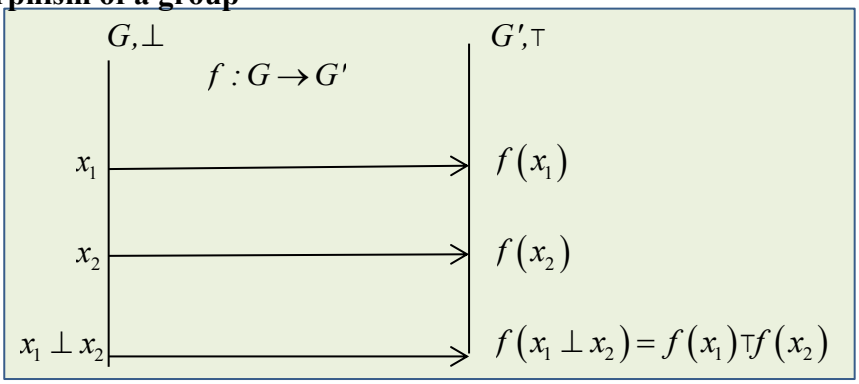
Any field finite is commutative.
The field of the remainders classes modulo p is commutative.

$$a=\frac{a}{1};\ \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd};\ \frac{a}{b}+\frac{c}{d}=\frac{ac}{bd}$$

It is admitted that a field contains at least two distinct elements

	Random function	Injective function	Surjective function	Bijective function
$E,*\to F,0$	morphism	Mono morphism	epimorphism	Isomorphism
$E,*\to F,0$	endomorphism			automorphism

Isomorphism of a group



Function $f:G\to G'$ is bijective

Definition

Let G a group whose rule is denoted $\perp$ and G' a group whose rule is $\top$. An application $f:G\to G'$ is called isomorphism if:

a) The function is bijective

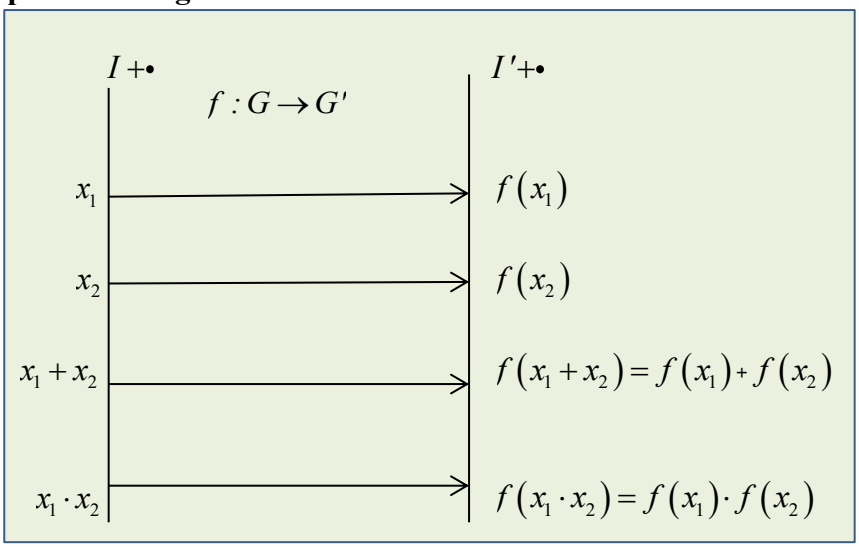
b) $f(x_1\perp x_2)=f(x_1)\top f(x_2)$

Then

$$f(e)=e'$$

$$f(x^{-1})=\left[f(x)\right]^{-1}$$

Isomorphism of ring



and the function $f:I\to I'$ is bijective then

- $f(0)=0$
- $f(x_1+x_2+...+x_n)=f(x_1)+f(x_2)+...+f(x_n)$
- $f(x_1+x_2+...+x_n)=f(x_1)+f(x_2)+...+f(x_n)$
- If I admits as unity element 1, then $f(1)$ is an unity element in 1

Isomorphism of field

The same concept as for an isomorphism of a ring

The identical groups from algebraic point of view are two groups of a different nature, when their elements can be grouped two by two, such that any algebraic relation between the elements of the first group is true simultaneously with the relation obtained by substituting the elements of the first group with those of the second group.

Morphism of $E:F$

Given two sets E,F with the composition rules $*,\circ$, we call morphism of the set E in the set F, any application in which the result of the composite of any two elements from E using the rule $*$ has as image in F through f the composite through $\circ$ of the corresponding images of the elements considered in E

Table of a group G

$\perp$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Theorem (C. Ionescu-Tiu)

If $P(x) \vdots a_0x^n + ... + a_n$ and $P'(x) \vdots a_0x^n + ... + a_n$, then $P(x) \vdots (a_0x^n + ... + a_n)^2$

Stolg-Cesaro's Lemma

If b_n is strictly monotone, endless then the following are true:

$$\lim_{n\to\infty} \sqrt[n]{a_n} = \lim_{n\to\infty} \frac{a_{n+1}}{a_n}$$

$$\lim_{n\to\infty} \sqrt[n]{a_1a_2...a_n} = \lim_{n\to\infty} \frac{a_1 + a_2 + ... + a_n}{n}$$

The formulae of the composed radicals

$$\sqrt{a+\sqrt{b}} = \sqrt{\frac{a+\sqrt{a^2-b}}{2}} + \sqrt{\frac{a-\sqrt{a^2-b}}{2}}$$

$$\sqrt{a-\sqrt{b}} = \sqrt{\frac{a+\sqrt{a^2-b}}{2}} - \sqrt{\frac{a-\sqrt{a^2-b}}{2}}$$

Harmonic division

$$A,B,C,D: \text{ if } \frac{CA}{CB} \cdot \frac{DB}{DA} = 1$$

$$max(x,y) = \frac{x+y+|x-y|}{2};$$

$$min(x,y) = \frac{x+y-|x-y|}{2}$$

Jensen's inequality

$$f_{convex} \Rightarrow f\left(\frac{\sum_1^n x_i}{n}\right) \le \frac{1}{n}\sum_1^n x_i$$

$$f_{concave} \Rightarrow f\left(\frac{\sum_{1}^{n} x_i}{n}\right) \geq \frac{1}{n}\sum_{1}^{n} x_i$$

Chapter Fi□e: Tri□ono□ etry

Sexagesimal degrees

A Sexagesimal degree is equal to the 90^{th} part of a right angle
The Sexagesimal minute is equal to the 60^{th} part from a sexagesimal degree.
The sexagesimal second is equal to the 60thpart from a sexagesimal minute.

Centesimal degrees

A centesimal degree is equal to the 100^{th} part from a right angle
The centesimal minute is equal to the 100^{th} part from a centesimal degree
The centesimal second is the 100^{th} part of a centesimal minute.

The radian

The measure in radians is the ratio between the lengths of the arc of a circle, which corresponds to an angle in the center, and the length of the circle's radius $\frac{l}{r}$.

One radian is the angle whose vertex is in the center of a circle that corresponds to an arc whose length is equal to the length of the circle's radius.

How to transform a measure to another one:

$$\frac{\alpha}{180°} = \frac{a'}{200^g} = \frac{a}{\pi}$$

$\alpha°$	0°	30°	45°	60°	90°	180°	270°	360°
a	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$	2π

Oriented plane

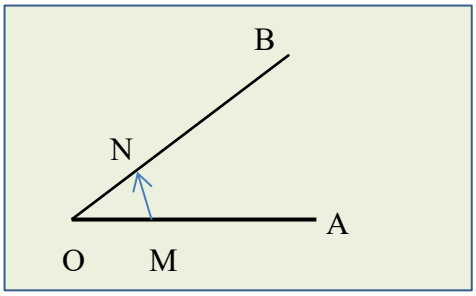
An oriented plane is a plane in which it has been established the positive direction for rotations.

Oriented angle

An oriented angle is the angle for which has been established the rotation direction.

The rotation direction (sense) ca be:

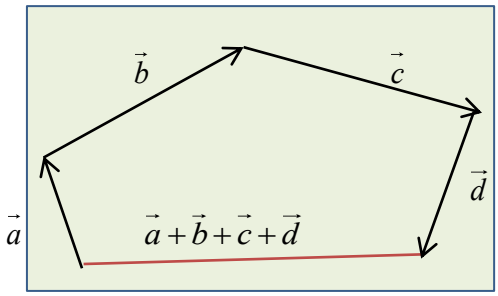
- Positive (direct or trigonometric) – is the sense inverse to the clock rotation
- Negative (retrograde) – is the sense of the clock rotation.



OA - The initial side
OB - The final side
M - The origin of the arc
N - The extremity of the arc

The rotation sense from OA to OB is considered the positive sense

To sum several vectors is used the polygon rule: To construct the sum of several vectors we will construct equal vectors with the given ones, such that the origin of one vector will coincide with the extremity of the precedent one. The vector that coincides with the origin of the first term, and the extremity will coincide with the origin of the last term, represents the sum of the considered vectors.

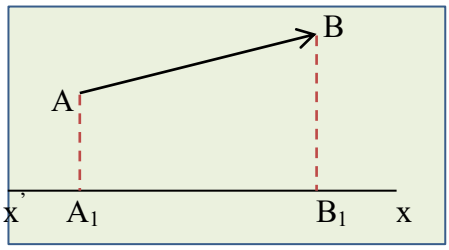


The product between a vector and a number

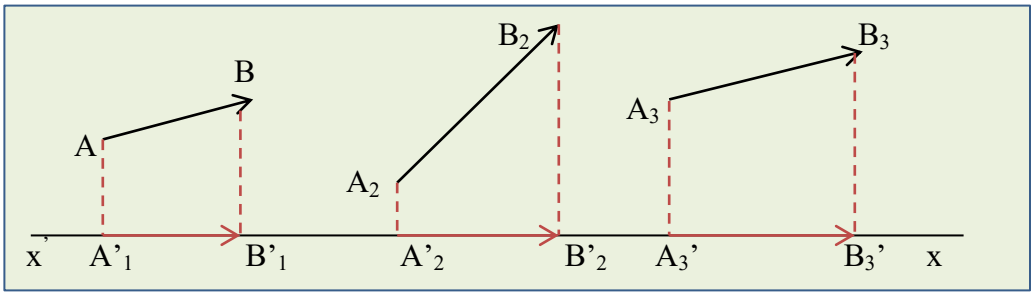
By multiplying a vector $\vec{a}$ with a real number λ, we obtain a vector which has its module equal to the product between the module of the number λ and the module of the vector $\vec{a}$, and the sense will be that of $\vec{a}$ or $-\vec{a}$, depending the sign of λ ($\lambda>0$, or $\lambda<0$); for $\lambda=0$, the product will be the null vector.

The projection of a vector on axis.

The projection of vector $\overrightarrow{AB}$ on axis x is the size of the vector $\overrightarrow{A_1B_1}$ and is denoted: $pr.x\overrightarrow{AB}$



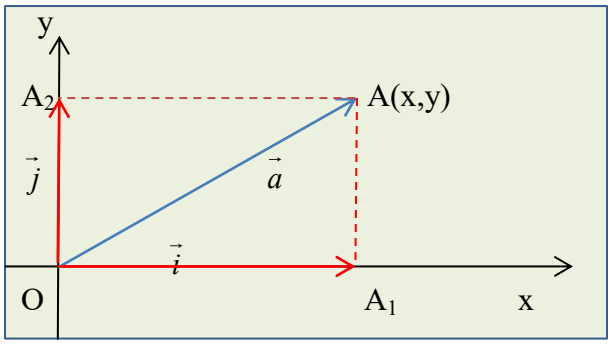
The projections of some vectors which have the same sense, on an axis, are proportional to their module.



$$\frac{A_1'B_1'}{\overrightarrow{A_1B_1}} = \frac{A_2'B_2'}{\overrightarrow{A_2B_2}} = \frac{A_3'B_3'}{\overrightarrow{A_3B_3}}$$

The decomposition of vectors in the plane

$$\vec{a} = \overrightarrow{xi} + \overrightarrow{yj}$$



$\vec{i}$ and $\vec{j}$ are the versors of the axes.

A versor is the vector whose module is equal to the unity.

Two angles that have the same size are equal.

The sum of two angles is the angle whose size is equal to the sum of the sizes of the two angles.

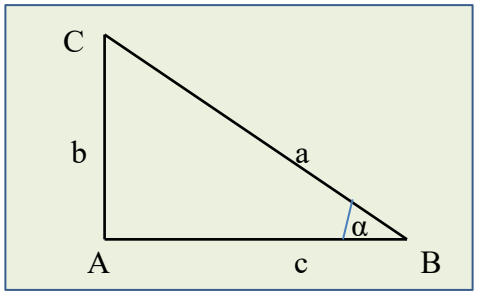
Between the set of real numbers and the set of oriented angles there is a bi-univocal correspondence.

Between the final position of an oriented angle and the set of the real numbers does not exist a bi-univocal correspondence; to a final position of the final side corresponds an infinity of angles that have various values.

Trigonometric functions of an acute angle

The sine

The sine of an acute angle is the ratio between the opposite cathetus and the hypothesis:



$$sin\,\alpha = \frac{b}{a}$$

The cosine

The cosine of an acute angle is the ratio between the adjoin cathetus and the hypotenuse.

$$cos\,\alpha = \frac{c}{a}$$

The tangent

The tangent of an acute angle is the ratio between the opposite cathetus and the adjoin cathetus of the angle:

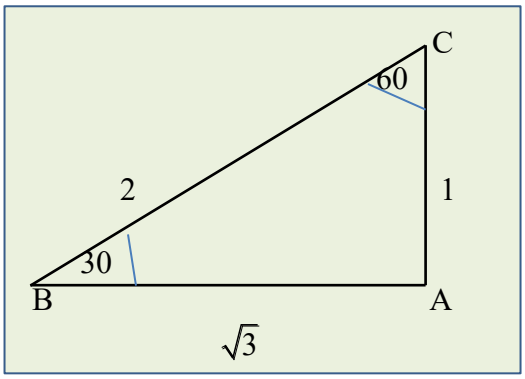
$$tan\,\alpha = \frac{b}{c}$$

The cotangent

The cotangent of an acute angle is the ratio between the adjoin cathetus and the opposite cathetus of the angle:

$$cot\,\alpha = \frac{c}{b}$$

The values of the trigonometric functions for angles: 30 , 45 , 60



$$\sin 30° = \frac{1}{2}$$

$$\cos 30° = \frac{\sqrt{3}}{2}$$

$$\tan 30° = \frac{1}{\sqrt{3}}$$

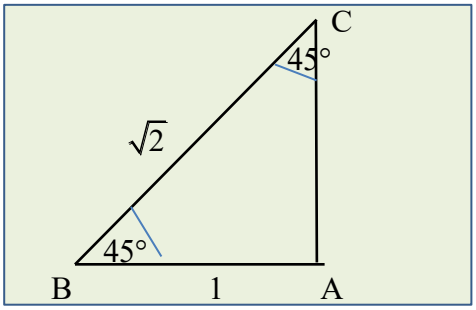
$$\cot 30° = \sqrt{3}$$

$$\sin 60° = \frac{\sqrt{3}}{2}$$

$$\cos 60° = \frac{1}{2}$$

$$\tan 60° = \sqrt{3}$$

$$\cot 60° = \frac{1}{\sqrt{3}} = \frac{\sqrt{3}}{3}$$



$$\sin 45° = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$$

$$\cos 45° = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$$

$$\tan 45° = 1$$

$$\cot 45° = 1$$

$$\frac{z_1}{z_2} = -\frac{\rho_1}{\rho_2}\left[\cos\left(\varphi_1 - \varphi_1\right) + i\sin\left(\varphi_1 - \varphi_1\right)\right]$$

The power of the complex numbers

The Moivre's formula

$$\left|z^n\right| = |z|^n;\ arg\left(z^n\right) = arg\left(nz\right)$$

$$z^n = \rho^n\left(\cos n\varphi + i\sin n\varphi\right);\left(\ n \in \mathbb{Z}\right)$$

The root of the n order from a complex number

$$\left|\sqrt[n]{z}\right| = |z|^{\frac{1}{n}};\ arg\sqrt[n]{z} = \frac{arg\, z + 2k\pi}{n};\ \left(k = 0,1,2,...,n-1\right)$$

Binomial equations

A binomial equation is an equation of the form:

$$z^n + \alpha = 0$$

where α is a complex number and z is the unknown, $(z \in \mathbb{R})$.

Example"

Find the solution for the following binomial equation:

$$\left(\frac{1+iz}{1-iz}\right)^4 = \frac{\frac{1}{2}+\frac{\sqrt{3}}{2}i}{\frac{1}{2}-\frac{\sqrt{3}}{2}i}$$

$$\rho_1 = \sqrt{\frac{1}{4}+\frac{3}{4}} = 1$$

$$tg\varphi_1 = \frac{\sqrt{3}}{2}\cdot\frac{2}{1} = \sqrt{3} \Rightarrow \varphi_1 = \frac{\pi}{3}$$

$$z_1 = \frac{1}{2}+\frac{\sqrt{3}}{2}i = cos\frac{\pi}{3} + i\,sin\frac{\pi}{3}$$

$$\rho_2 = \sqrt{\frac{1}{4}+\frac{3}{4}} = 1$$

$$arg\,z_2 = 2\pi - arg\,z_1 = 2\pi - \frac{\pi}{3} = \frac{5\pi}{3} = \varphi_2$$

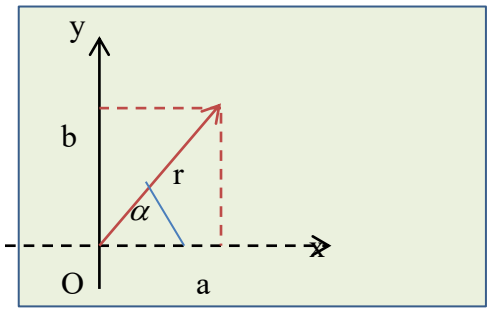
$$z_2 = \frac{1}{2}-\frac{\sqrt{3}}{2}i = cos\frac{5\pi}{3} + i\,sin\frac{5\pi}{3}$$

$$\frac{z_1}{z_2} = cos\left(\frac{-4\pi}{3}\right) + i\,sin\left(\frac{-4\pi}{3}\right) = cos\frac{4\pi}{3} - i\,sin\frac{4\pi}{3} = cos\frac{2\pi}{3} + i\,sin\frac{2\pi}{3}$$

$$\frac{1+iz}{1-iz} = \sqrt[4]{cos\frac{2\pi}{3} + i\,sin\frac{2\pi}{3}} = cos\frac{\frac{2\pi}{3}+2k\pi}{4} + i\,sin\frac{\frac{2\pi}{3}+2k\pi}{4}$$

The trigonometric functions of an orientated angle

The sine of an angle α is the ratio between the projection of a vector radius on the y-axis and its module: $sin\,\alpha = \frac{b}{r}$



The cosine of an angle α is the ratio between the projection of a vector radius on the x-axis and its module $cos\,\alpha = \frac{a}{r}$

The tangent of an angle α is the ratio between the projection of a vector radius on the y-axis and its projection on the x-radius: $tan\,\alpha = \frac{b}{a}$.

The cotangent of an angle α is the ratio between the projection of a vector radius on the x-axis and its projection on the y-radius:. $cot\,\alpha = \frac{a}{b}$

The secant of an angle α is the ratio between the vector radius and it projection on the x-axis: $sec\,\alpha = \frac{r}{a}$

The cosecant of an angle α is the ratio between the vector radius and its projection on the y-axis: $csc\,\alpha = \frac{r}{b}$

The signs of the trigonometric functions

	Quadrant I	Quadrant II	Quadrant III	Quadrant IV
sin α	+	+	-	-
cos α	+	-	-	+
tan α	+	-	+	-
cot α	+	-	+	-
sec α	+	-	-	+
csc α	+	+	-	-

Or

+	+
-	-

$\sin\alpha$
$\sec\alpha$

+	+
-	-

cos α
csc α

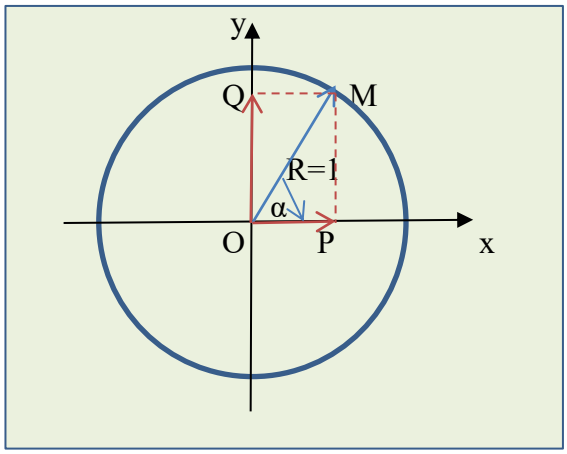
+	+
-	-

tan α
cot α

Trigonometric circle

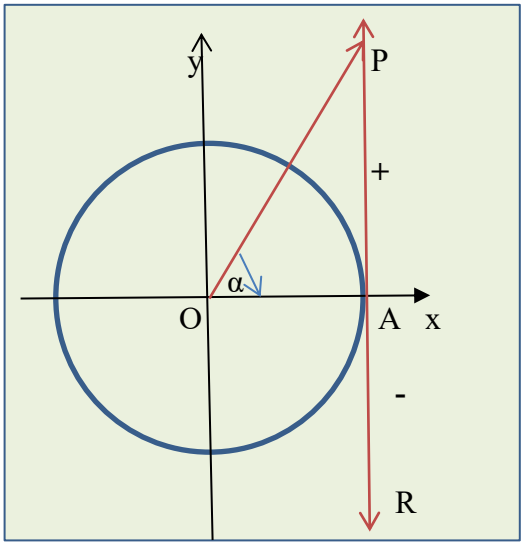
A trigonometric circle is a circle whose radius $R = 1$ (the unity) and with the center in the origin of the coordinate axes.

1. The sine of an angle is equal to the projection of the vector radius on the x-axis
2. The cosine of an angle is equal to the projection of the vector radius on the y-axis

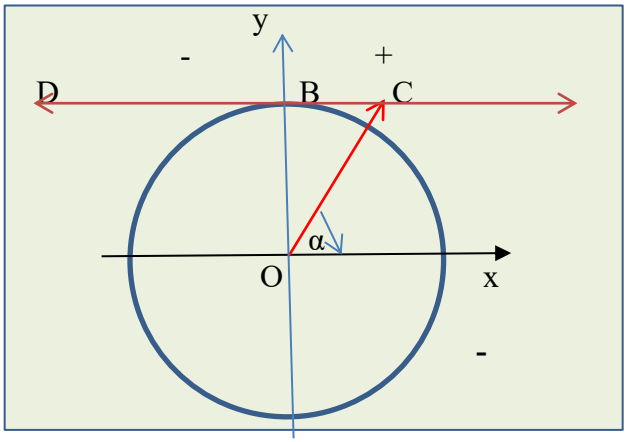


3. The tangent of an angle is equal to the projection of the vector radius on the tangent axis

PR is the tangent axis (the tangent to the circle $C(O)$ in the point A)



4. The cotangent of an angle is equal to the projection of the vector radius on the cotangent axis.



CD is the cotangent axis (is the tangent to the circle $C(O)$ in the point B)

$sin\,90° = 1$ $cos\,90° = 0$ $tan\,90°$ there is none

$sin\,180° = 0$ $cos\,180° = -1$ $tan\,180° = 0$

$sin\,270° = -1$ $cos\,270° = 0$ $tan\,270°$ there is none

$sin\,360° = 0$ $cos\,360° = 1$ $tan\,360° = 0$

$cot\,90° = 0$

$cot\,180°$ there is none

$cot\,270° = 0$

$cot\,360°$ there is none

The reduction to an acute angle $\alpha \le 45°$

$$sin(90° - \alpha) = cos\,\alpha \qquad sin(90° + \alpha) = cos\,\alpha$$
$$cos(90° - \alpha) = sin\,\alpha \qquad cos(90° + \alpha) = -sin\,\alpha$$
$$tan(90° - \alpha) = cot\,\alpha \qquad tan(90° + \alpha) = -cot\,\alpha$$
$$cot(90° - \alpha) = tan\,\alpha \qquad cot(90° + \alpha) = -tan\,\alpha$$

$$sin(180° - \alpha) = sin\,\alpha \qquad sin(180° + \alpha) = -sin\,\alpha$$
$$cos(180° - \alpha) = -cos\,\alpha \qquad cos(180° + \alpha) = -cos\,\alpha$$
$$tan(180° - \alpha) = tan\,\alpha \qquad tan(180° + \alpha) = tan\,\alpha$$
$$cot(180° - \alpha) = -cot\,\alpha \qquad cot(180° + \alpha) = cot\,\alpha$$

$$sin(270° - \alpha) = -cos\,\alpha \qquad sin(270° + \alpha) = -cos\,\alpha$$
$$cos(270° - \alpha) = -sin\,\alpha \qquad cos(270° + \alpha) = sin\,\alpha$$
$$tan(270° - \alpha) = cot\,\alpha \qquad tan(270° + \alpha) = -cot\,\alpha$$
$$cot(270° - \alpha) = tan\,\alpha \qquad cot(270° + \alpha) = -tan\,\alpha$$

$$sin(360° - \alpha) = -sin\,\alpha \qquad sin(-\alpha) = -sin\,\alpha$$
$$cos(360° - \alpha) = cos\,\alpha \qquad cos(-\alpha) = cos\alpha$$
$$tan(360° - \alpha) = -tan\,\alpha \qquad tan(-\alpha) = -tan\,\alpha$$
$$cot(360° - \alpha) = -cot\,\alpha \qquad cot(-\alpha) = -cot\,\alpha$$

Periodic fractions

A function $f(x)$ is called periodic if there is a number $T \neq 0$, such that for any x belonging to its domain of definition, the function's values in the $x+T$ and x are equal: $f(x+T)=f(x)$.

The number T is called the period of the function $f(x)$.

Theorem

If the number T is the period for the function $f(x)$, then the numbers kT $(k=\pm 1,\pm 2,...)$ also are periods for the given function.

Principal period

The principal period is the smaller positive period of a period function (frequently the principal period is called shortly: the period).

The functions $\sin x$ and $\cos x$ have 2π as principal period, and the functions $\tan x$ and $\cot x$ have π as principal period.

The principal period of function $f(x)=a\sin(\omega x+\varphi)$, where a and ω are constants non-null, is equal to $\frac{2\pi}{\omega}$

The harmonic simple oscillation: $|a|$ is the amplitude, ω is the pulsation and φ is the phase difference of the oscillation.

Periodic functions odd and even

The function $f(x)$ is even if for any x belonging to its domain of definition, is satisfied the following relation:

$$f(x)=f(x)$$

The function $f(x)$ is odd if for any x belonging to its domain of definition, is satisfied the following relation:

$$f(-x)=-f(x)$$

Theorem

The graph of an even function is symmetric relative to the x-axis, and the graph of the odd functions is symmetric relative to the y-axis.

$\cos(-x)=\cos x$ -even

$$\left.\begin{aligned}&\sin(-x)=-\sin x\\&\tan(-x)=-\tan x\\&\cot(-x)=-\cot x\end{aligned}\right\}\ \text{odd}$$

There are functions which are neither odd nor even.

Strict monotone functions

1. If $f(x_1) < f(x_2)$ for any $x_1 < x_2$, then the function is called strictly increasing on the interval $[a,b]$.
2. If $f(x_1) > f(x_2)$ for any $x_1 < x_2$, then the function is called strictly decreasing on the interval $[a,b]$.

A function strictly increasing or decreasing on an interval is called a strictly monotone function on that interval.

The monotony intervals of the trigonometric functions

Function $\sin x$

0	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$	2π
$0 \nearrow\nearrow$	$1 \searrow\searrow$	0	$\searrow\searrow -1 \nearrow\nearrow$	0

Function $\cos x$

0	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$	2π
$1 \searrow\searrow$	$0 \searrow\searrow$	-1	$\nearrow\nearrow 0 \nearrow\nearrow$	1

Function $\tan x$

0	$\frac{\pi}{2}$	π
$0 \nearrow\nearrow$	$+\infty \searrow\searrow$	0

Function $\cot x$

0	$\frac{\pi}{2}$	π
$+\infty \searrow\searrow$	$0 \searrow\searrow$	$-\infty$

The domains of definition and the set of values for the trigonometric functions

$\sin x : \mathbb{R} \to [-1,+1]$

$\cos x : \mathbb{R} \to [-1,+1]$

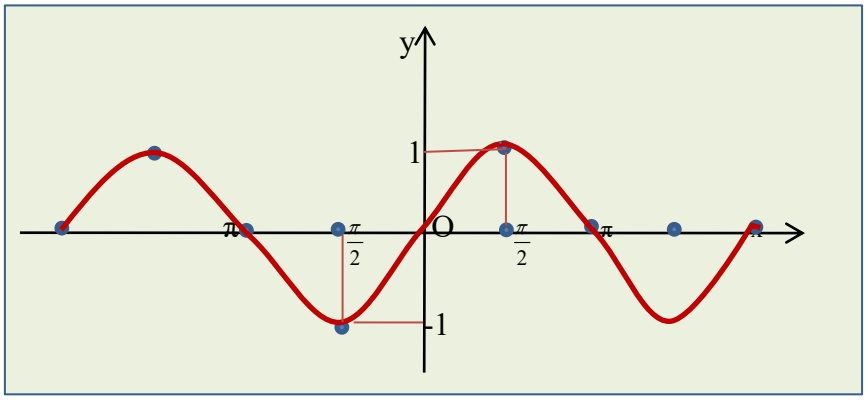
$\tan x : \mathbb{R} - \left\{ \frac{\pi}{2} + k\pi, k \in \mathbb{Z} \right\} \to \mathbb{R}$

$\cot x : \mathbb{R} - \{k\pi, k \in \mathbb{Z}\} \to \mathbb{R}$

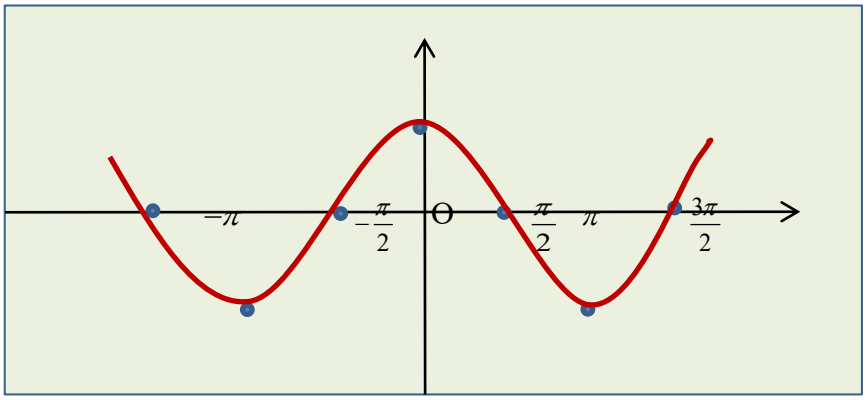
The graphics of the trigonometric functions

The graphics of $\sin x,\ \cos x$ are called sinusoidal

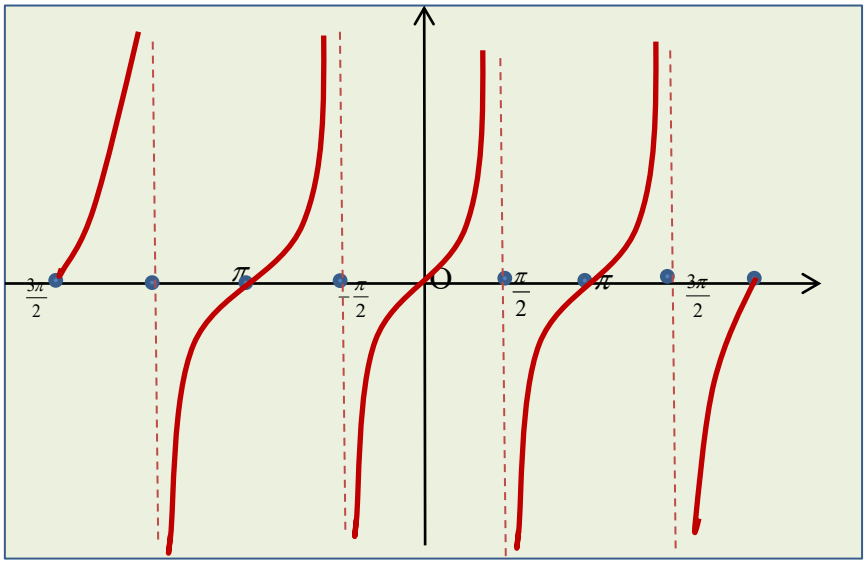
1. $f(x) = \sin x$



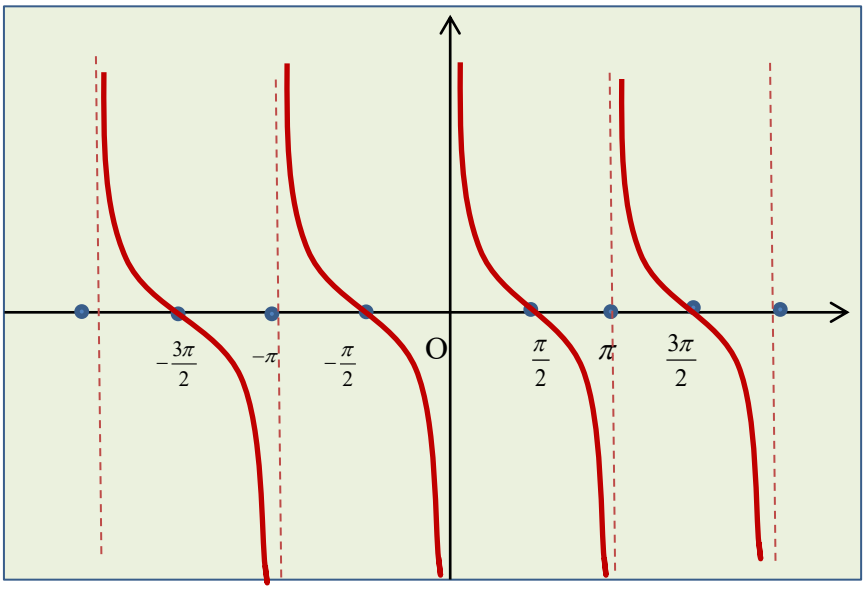
2. $f(x) = \cos x$



3. $f(x) = \tan x$



4. $f(x) = \cot x$

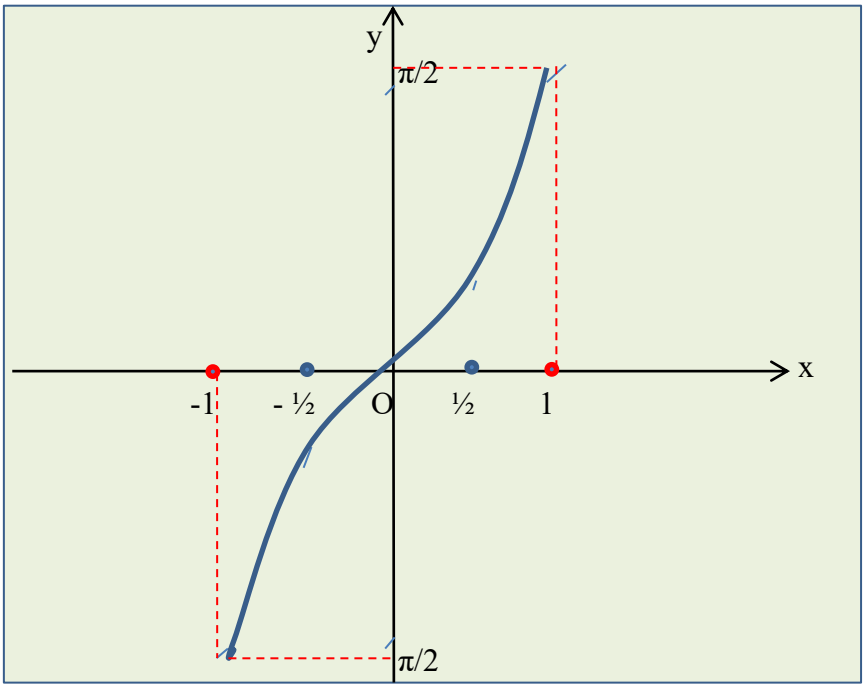


Trigonometric functions inverse

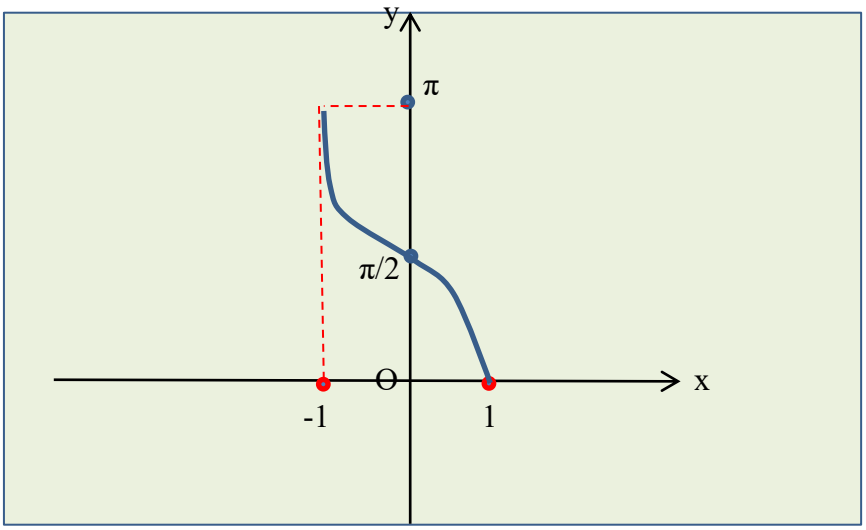
Any function which is strictly monotone on an interval can be inversed; the domain of definition and the set of the values of the function will be respectively the set of the values and the domain of definition of the inverse function.

If a function is strict increasing (strict decreasing) on an interval, then the inverse function will be also strict increasing (strict decreasing) on that interval.

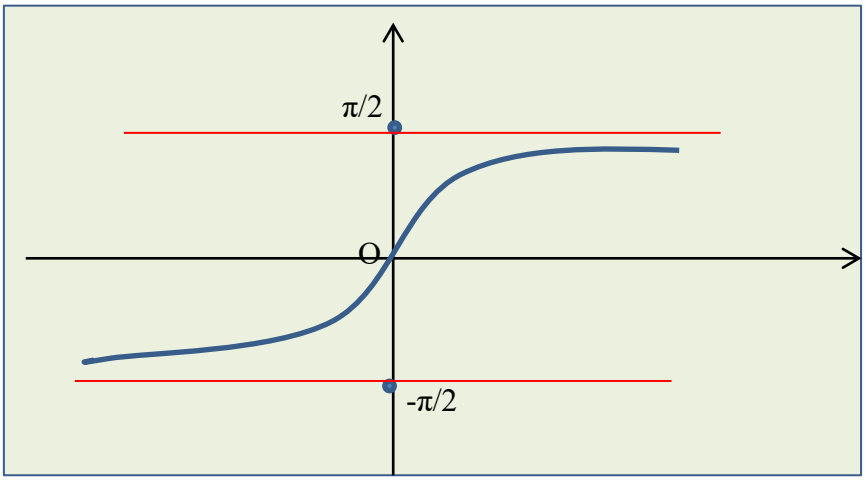
Function *arcsin x*



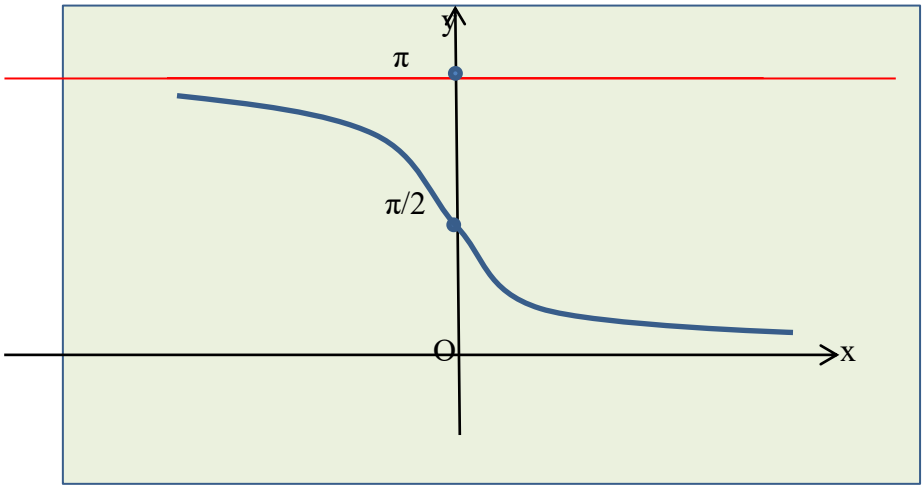
Function *arccos x*



Function *arctan x*



Function *arc cot x*



Fundamental formulae

	$\sin\alpha$	$\cos\alpha$	$\tan\alpha$	$\cot\alpha$	$\sec\alpha$	$\csc\alpha$
$\sin\alpha$		$\pm\sqrt{1-\cos^2\alpha}$	$\frac{\tan\alpha}{\pm\sqrt{1+\tan^2\alpha}}$	$\frac{1}{\pm\sqrt{1+\cot^2\alpha}}$	$\pm\sqrt{1-\frac{1}{\sec^2\alpha}}$	$\frac{1}{\csc\alpha}$
$\cos\alpha$	$\pm\sqrt{1-\sin^2\alpha}$		$\frac{1}{\pm\sqrt{1+\tan^2\alpha}}$	$\frac{\cot\alpha}{\pm\sqrt{1+\cot^2\alpha}}$	$\frac{1}{\sec\alpha}$	$\pm\sqrt{1-\frac{1}{\csc^2\alpha-1}}$
$\tan\alpha$	$\frac{\sin\alpha}{\pm\sqrt{1-\sin^2\alpha}}$	$\frac{\pm\sqrt{1-\cos^2\alpha}}{\cos\alpha}$		$\frac{1}{\cot\alpha}$	$\pm\sqrt{\sec^2\alpha-1}$	$\pm\frac{1}{\sqrt{\csc^2\alpha-1}}$
$\cot\alpha$	$\frac{\pm\sqrt{1-\sin^2\alpha}}{\sin\alpha}$	$\frac{\cos\alpha}{\pm\sqrt{1-\cos^2\alpha}}$	$\frac{1}{\tan\alpha}$		$\pm\sqrt{\frac{1}{\sec^2\alpha-1}}$	$\pm\sqrt{\csc^2\alpha-1}$
$\sec\alpha$	$\frac{1}{\pm\sqrt{1-\sin^2\alpha}}$	$\frac{1}{\cos\alpha}$	$\pm\sqrt{1+\tan^2\alpha}$	$\frac{\pm\sqrt{1+\csc^2\alpha}}{\csc\alpha}$		$\frac{1}{\pm\sqrt{1-\frac{1}{\csc^2\alpha-1}}}$
$\csc\alpha$	$\frac{1}{\sin\alpha}$	$\frac{1}{\pm\sqrt{1-\cos^2\alpha}}$	$\frac{\pm\sqrt{1+\tan^2\alpha}}{\tan\alpha}$	$\pm\sqrt{1+\cot^2\alpha}$	$\frac{1}{\pm\sqrt{1-\frac{1}{\sec^2\alpha-1}}}$	

$$\sin^2\alpha+\cos^2\alpha=1$$

$$\tan\alpha=\frac{\sin\alpha}{\cos\alpha}$$

$$\cot\alpha=\frac{\cos\alpha}{\sin\alpha}$$

$$\tan\alpha\cdot\cot\alpha=1$$

$$1-\cos\alpha=2\sin^2\frac{\alpha}{2}$$

$$1+\cos\alpha=2\cos^2\frac{\alpha}{2}$$

$$\sin^2\frac{\alpha}{2}=\frac{1-\cos\alpha}{2}$$

$$\cos^2\frac{\alpha}{2}=\frac{1+\cos\alpha}{2}$$

$$1 - \sin 2\alpha = (\sin\alpha - \cos\alpha)^2$$

$$1 + \sin 2\alpha = (\sin\alpha + \cos\alpha)^2$$

$$\sec\alpha = \frac{1}{\cos\alpha}$$

$$\csc\alpha = \frac{1}{\sin\alpha}$$

$$\sin\alpha \sin\beta = \frac{\cos(\alpha - \beta) - \cos(\alpha + \beta)}{2}$$

$$\cos\alpha \cos\beta = \frac{\cos(\alpha + \beta) + \cos(\alpha - \beta)}{2}$$

$$\sin\alpha \cos\beta = \frac{\sin(\alpha + \beta) + \sin(\alpha - \beta)}{2}$$

$$\tan\alpha \tan\beta = \frac{\tan\alpha + \tan\beta}{\cot\alpha + \cot\beta}$$

$$\sin(\alpha + \beta) = \sin\alpha \cos\beta + \sin\beta \cos\alpha$$

$$\sin(\alpha - \beta) = \sin\alpha \cos\beta - \sin\beta \cos\alpha$$

$$\cos(\alpha + \beta) = \cos\alpha \cos\beta - \sin\alpha \sin\beta$$

$$\cos(\alpha - \beta) = \cos\alpha \cos\beta + \sin\alpha \sin\beta$$

$$\tan(\alpha + \beta) = \frac{\tan\alpha + \tan\beta}{1 - \tan\alpha \tan\beta}$$

$$\tan(\alpha - \beta) = \frac{\tan\alpha - \tan\beta}{1 + \tan\alpha \tan\beta}$$

$$\cot(\alpha + \beta) = \frac{\cot\alpha \cot\beta - 1}{\cot\alpha + \cot\beta}$$

$$\cot(\alpha - \beta) = \frac{\cot\alpha \cot\beta + 1}{-\cot\alpha + \cot\beta}$$

$l = ar$

l is the lengths of the circle's arc

a is the measure in radian of the angle with the vertex in the center of the circle

r is the circle's radius.

$\omega = \frac{2\pi}{T}$; $\alpha = \omega t$

ω is he angular speed (in the circular and uniform movement)

t is the time

α is the angle

The trigonometric functions of a sum of three angles

$$sin(\alpha_1+\alpha_2+\alpha_3)=sin\alpha_1 cos\alpha_2 cos\alpha_3+sin\alpha_2 cos\alpha_1 cos\alpha_3+sin\alpha_3 cos\alpha_1 cos\alpha_2-sin\alpha_1 sin\alpha_2 sin\alpha_3$$

$$cos(\alpha_1+\alpha_2+\alpha_3)=cos\alpha_1 cos\alpha_2 cos\alpha_3-sin\alpha_1 sin\alpha_2 cos\alpha_3-sin\alpha_1 sin\alpha_3 cos\alpha_2-sin\alpha_3 sin\alpha_2 cos\alpha_1$$

$$tan(\alpha_1+\alpha_2+\alpha_3)=\frac{tan\alpha_1+tan\alpha_2+tan\alpha_3-tan\alpha_1 tan\alpha_2 tan\alpha_3}{1-tan\alpha_1 tan\alpha_2-tan\alpha_1 tan\alpha_3-tan\alpha_2 tan\alpha_3}$$

$$cot(\alpha_1+\alpha_2+\alpha_3)=\frac{cot\alpha_1 cot\alpha_2 cot\alpha_3-cot\alpha_1-cot\alpha_2-cot\alpha_3}{cot\alpha_1 cot\alpha_2+cot\alpha_1 cot\alpha_3+cot\alpha_2 cot\alpha_3-1}$$

The trigonometric functions of a double-angle

$$sin2\alpha=2sin\alpha cos\alpha$$

$$cos2\alpha=cos^2\alpha-sin^2\alpha=1-2sin^2\alpha=2cos^2\alpha-1$$

$$tan2\alpha=\frac{2tan\alpha}{1-tan^2\alpha}$$

$$cot2\alpha=\frac{cot^2\alpha-1}{2cot\alpha}$$

The trigonometric functions of a triple-angle

$$sin3\alpha=sin\alpha(3-4sin^2\alpha)=3sin\alpha-4sin^3\alpha$$

$$cos3\alpha=cos\alpha(4cos^2\alpha-3)=4cos^3\alpha-3cos\alpha$$

$$tan3\alpha=\frac{3tan\alpha-tan^3\alpha}{1-3tan^2\alpha}$$

$$cot3\alpha=\frac{cot^3\alpha-3cot\alpha}{3cot^2\alpha-1}$$

The trigonometric functions of a half-angle

$$sin\frac{\alpha}{2}=\pm\sqrt{\frac{1-cos\alpha}{2}}$$

$$cos\frac{\alpha}{2}=\pm\sqrt{\frac{1+cos\alpha}{2}}$$

$$an\frac{\alpha}{2}=\pm\sqrt{\frac{1-cos\alpha}{1+cos\alpha}}=\frac{sin\alpha}{1+cos\alpha}=\frac{1-cos\alpha}{sin\alpha}$$

$$cot\frac{\alpha}{2}=\pm\sqrt{\frac{1+cos\alpha}{1-cos\alpha}}=\frac{1+cos\alpha}{sin\alpha}=\frac{sin\alpha}{1-cos\alpha}$$

The trigonometric functions of an angle α in function of $tan\frac{\alpha}{2}=t$

$$sin\alpha=\frac{2t}{1+t^2}$$

$$\cos\alpha = \frac{1-t^2}{1+t^2}$$
$$\tan\alpha = \frac{2t}{1-t^2},$$
$$\cot\alpha = \frac{1-t^2}{2t}$$

Transformation of sums of trigonometric functions in products

$$\sin p + \sin q = 2\sin\frac{p+q}{2}\cos\frac{p-q}{2}$$
$$\sin p - \sin q = 2\sin\frac{p-q}{2}\cos\frac{p+q}{2}$$
$$\cos p + \cos q = 2\cos\frac{p+q}{2}\cos\frac{p-q}{2}$$
$$\cos p - \cos q = 2\sin\frac{q+p}{2}\sin\frac{q-p}{2}$$
$$\tan p + \tan q = \frac{\sin(p+q)}{\cos p\cos q}$$
$$\tan p - \tan q = \frac{\sin(p-q)}{\cos p\cos q}$$
$$\cot p + \cot q = \frac{\sin(p+q)}{\cos p\cos q}$$
$$\cot p - \cot q = \frac{\sin(q-p)}{\sin p\sin q}$$

Transformation of products of trigonometric functions in sums

$$\sin\alpha\sin\beta = \frac{\cos(\alpha-\beta)-\cos(\alpha+\beta)}{2}$$
$$\sin\alpha\cos\beta = \frac{\sin(\alpha+\beta)+\sin(\alpha-\beta)}{2}$$
$$\cos\alpha\cos\beta = \frac{\cos(\alpha+\beta)+\cos(\alpha-\beta)}{2}$$

Relations between the arc functions

$$\arcsin x + \arccos x = \frac{\pi}{2}$$
$$\arctan x + \operatorname{arccot} x = \frac{\pi}{2}$$

$$\sin\left(\arcsin x\right) = x$$
$$\sin\left(\arccos x\right) = \sqrt{1-x^2}$$
$$\sin\left(\arctan x\right) = \frac{x}{\sqrt{1+x^2}}$$
$$\sin\left(\operatorname{arccot} x\right) = \frac{1}{\sqrt{1+x^2}}$$
$$\cos\left(\arccos x\right) = x$$
$$\cos\left(\arcsin x\right) = \sqrt{1-x^2}$$
$$\cos\left(\arctan x\right) = \frac{1}{\sqrt{1+x^2}}$$
$$\cos\left(\operatorname{arccot} x\right) = \frac{x}{\sqrt{1+x^2}}$$

$$\tan\left(\arctan x\right) = x$$
$$\tan\left(\arcsin x\right) = \frac{x}{\sqrt{1-x^2}}$$
$$\tan\left(\arccos x\right) = \frac{\sqrt{1-x^2}}{x}$$
$$\tan\left(\operatorname{arccot} x\right) = \frac{1}{x}$$
$$\cot\left(\operatorname{arccot} x\right) = x$$
$$\cot\left(\arcsin x\right) = \frac{\sqrt{1-x^2}}{x}$$
$$\cot\left(\arccos x\right) = \frac{x}{\sqrt{1-x^2}}$$
$$\cot\left(\arctan x\right) = \frac{1}{x}$$

$$\arcsin\left(\sin\alpha\right) = \alpha$$
$$\arccos\left(\cos\alpha\right) = \alpha$$
$$\arctan\left(\tan\alpha\right) = \alpha$$
$$\operatorname{arccot}\left(\cot\alpha\right) = \alpha$$

$$arcsin\left(cos\,\alpha\right)=\frac{\pi}{2}-\alpha$$

$$arccos\left(sin\,\alpha\right)=\frac{\pi}{2}-\alpha$$

$$arctan\left(cot\,\alpha\right)=\frac{\pi}{2}-\alpha$$

$$arc\,cot\left(tan\,\alpha\right)=\frac{\pi}{2}-\alpha$$

$$tan\,\alpha\,tan\,\beta=\frac{tan\,\alpha+tan\,\beta}{cot\,\alpha+cot\,\beta}$$

$$cot\,\alpha\,cot\,\beta=\frac{cot\,\alpha+cot\,\beta}{tan\,\alpha+tan\,\beta}$$

$$cot\,\alpha\,tan\,\beta=\frac{cot\,\alpha+tan\,\beta}{tan\,\alpha+cot\,\beta}$$

The computation of a sum of arc-functions

$$arcsin\,x+arcsin\,y=arcsin\left(x\sqrt{1-y^2}+y\sqrt{1-x^2}\right)$$

$$arcsin\,x-arcsin\,y=arcsin\left(x\sqrt{1-y^2}-y\sqrt{1-x^2}\right)$$

$$arccos\,x+arccos\,y=arccos\left(xy-\sqrt{1-x^2}\sqrt{1-y^2}\right)$$

$$arccos\,x-arccos\,y=arccos\left(xy+\sqrt{1-x^2}\sqrt{1-y^2}\right)$$

$$arctan\,x+arctan\,y=arctan\,\frac{x+y}{1-xy}$$

$$arctan\,x-arctan\,y=arctan\,\frac{x-y}{1+xy}$$

$$arc\,cot\,x+arc\,cot\,y=arc\,cot\,\frac{xy-1}{x+y}$$

$$arc\,cot\,x-arc\,cot\,y=arc\,cot\,\frac{xy+1}{x-y}$$

Trigonometric sums

$$S_1=sin\,a+sin\left(a+h\right)+...+sin\left[a+\left(n-1\right)h\right]=\frac{sin\frac{nh}{2}\,sin\left[a+\left(n-1\right)\frac{h}{2}\right]}{sin\frac{h}{2}}$$

$$S_2 = \cos a + \cos(a+h) + \ldots + \cos\left[a + (n-1)h\right] = \frac{\sin\frac{nh}{2}\cos\left[a + (n-1)\frac{h}{2}\right]}{\sin\frac{h}{2}}$$

How is computed

$$S_2 + iS_2 = \cos a + \cos(a+h) + \ldots + \cos\left[a + (n-1)h\right] +$$

$$+ i\sin a + i\sin(a+h) + \ldots + i\sin\left[a + (n-1)h\right] =$$

$$= (\cos a + i\sin a) + \left[\cos(a+h) + i\sin(a+h)\right] + \ldots +$$

$$+ \left\{\cos\left[a + (n-1)\frac{h}{2}\right] + i\sin\left[a + (n-1)\frac{h}{2}\right]\right\} =$$

$$= (\cos a + i\sin a)\left\{1 + (\cosh + i\sinh)^1 + \ldots + (\cosh + i\sinh)^{n-1}\right\} =$$

$$= (\cos a + i\sin a)\frac{(\cosh + i\sinh)^n - 1}{(\cosh + i\sinh) - 1} = (\cos a + i\sin a)\frac{-2\sin^2 n\frac{h}{2} + i\sin n\frac{h}{2}}{-2\sin^2\frac{h}{2} + i2\sin\frac{h}{2}\cos\frac{h}{2}} =$$

$$= (\cos a + i\sin a)\frac{+2i\sin n\frac{h}{2}\left(i\sin n\frac{h}{2} + \cos n\frac{h}{2}\right)}{+2i\sin\frac{h}{2}\left(i\sin\frac{h}{2} + \cos\frac{h}{2}\right)} =$$

$$= (\cos a + i\sin a)\frac{\sin\frac{nh}{2}}{\sin\frac{h}{2}}\left(\cos\frac{n-1}{2}h + \sin\frac{n-1}{2}h\right) =$$

$$= \frac{\sin\frac{nh}{2}}{\sin\frac{h}{2}}\left[\cos\left(a + \frac{n-1}{2}h\right) + i\sin\left(a + \frac{n-1}{2}h\right)\right] =$$

$$= \frac{\sin\frac{nh}{2}}{\sin\frac{h}{2}}\cos\left(a + \frac{n-1}{2}h\right) + i\frac{\sin\frac{nh}{2}}{\sin\frac{h}{2}}\sin\left(a + \frac{n-1}{2}h\right)$$

Then,

$$\begin{cases} S_2 = \dfrac{\sin\frac{nh}{2}}{\sin\frac{h}{2}}\cos\left(a + \dfrac{n-1}{2}h\right) \\ S_1 = \dfrac{\sin\frac{nh}{2}}{\sin\frac{h}{2}}\sin\left(a + \dfrac{n-1}{2}h\right) \end{cases}$$

$$S_3 = \cos^2 x + \cos^2 2x + ... + \cos^2 nx = \frac{n}{2} + \frac{\sin nx \cos(n+1)x}{2\sin x}$$

$$S_4 = \sin^2 x + \sin^2 2x + ... + \sin^2 nx = \frac{n}{2} - \frac{\sin nx \cos(n+1)x}{2\sin x}$$

$$S_5 = \sin x + \sin 2x + ... + \sin nx = \frac{\sin\frac{nx}{2}}{\sin\frac{x}{2}} \sin\left(\frac{n+1}{2}x\right)$$

$$S_6 = \cos x + \cos 2x + ... + \cos nx = \frac{\sin\frac{nx}{2}}{\sin\frac{x}{2}} \cos\left(\frac{n+1}{2}x\right)$$

Trigonometric functions of multiple angles

$$\sin nx = C_n^1 \cos^{n-1} x \sin x - C_n^3 \cos^{n-3} x \sin^3 x + ...$$

$$\cos nx = C_n^0 \cos^n x - C_n^2 \cos^{n-2} x \sin^2 x + ...$$

$$\tan nx = \frac{C_n^1 \tan x - C_n^3 \tan^3 x + ..}{1 - C_n^2 \tan^2 x + ...}$$

$$\cot nx = \frac{C_n^0 \cot^n x - C_n^2 \cot^{n-2} x + ..}{C_n^1 \cot^{n-1} x - C_n^3 \cot^{n-3} x + ...}$$

The power of the trigonometric functions

I)

1) $$\sin^{2p} x = \frac{(-1)^p}{2^{2p-1}} \cdot$$

$$\cdot \left[\cos 2px - C_{2p}^1 \cos 2(p-1)x - C_{2p}^2 \cos 2(p-2)x + ... + (-1)^{p-1} C_{2p}^{p-1} \cos 2x\right] +$$

$$+ \frac{1}{2^{2p}} C_{2p}^p ;$$

2) $$\sin^{2p+1} x = \frac{(-1)^p}{2^{2p}} \cdot$$

$$\cdot \left[\sin(2p+1)x - C_{2p+1}^1 \sin(2p-1)x + C_{2p+1}^2 \sin(2p-3)x + ... + (-1)^p C_{2p+1}^p \sin x\right]$$

II)

1) $$\cos^{2p} x = \frac{1}{2^{2p-1}} \cdot$$

$$\cdot \left[\cos 2px + C_{2p}^1 \cos 2(p-1)x + C_{2p}^2 \cos 2(p-2)x + ... + C_{2p}^{p-1} \cos 2x\right] +$$

$$+ \frac{1}{2^{2p}} C_{2p}^p$$

2) $cos^{2p+1} x = \frac{1}{2^{2p}} \cdot$

$\cdot\left[cos(2p+1)x + C_{2p+1}^{1} cos(2p-1)x + C_{2p+1}^{2} cos(2p-3)x + ... + C_{2p+1}^{p} cos\, x\right]$

Trigonometric identity

A trigonometric identity is the equality which contains the trigonometric functions of one or more angles and it is true for all their admissible values.

Conditional identities

Conditional identities are two trigonometric expressions which are not equal for the whole set of admissible values of their angles, but for a subset of it (which will satisfy certain conditions).

Solved Problem

Prove that the identity: $sin(arccos\, x) = \sqrt{1-x^2}$.

The equality takes place for $|x| \le 1$.

We denote: $arccos\, x = \alpha$, then $0 \le \alpha \le \pi$, and therefore $sin\, \alpha \ge 0$.

But $|sin\, \alpha| = \sqrt{1-cos^2 \alpha} = \sqrt{1-cos^2 \alpha(arccos\, x)} = \sqrt{1-x^2}$, therefore $sin(arccos\, x) = \sqrt{1-x^2}$.

Trigonometric equations

$arcsin\, a = (-1)^k arcsin\, a + k\pi, \quad k \in \mathbb{Z}$

$arccos\, a = \pm arccos\, a + 2k\pi, \quad k \in \mathbb{Z}$

$arctan\, a = arctan\, a + k\pi, \quad k \in \mathbb{Z}$

$arc\, cot\, a = arc\, cot\, a + k\pi, \quad k \in \mathbb{Z}$

(The $arcsin\, a$ is the set of all angles whose sin is equal to a.

$arcsin\, a$ is the angle $\alpha \in \left[-\frac{\pi}{2}, +\frac{\pi}{2}\right]$ whose sin is equal to a)

A trigonometric equation is the equality which contains the unknown only under the sign of the trigonometric function and which is true only for certain values of the unknown.

I. Trigonometric equations elementary

$sin\, x = a \Rightarrow x = (-1)^k arcsin\, a + k\pi \quad (k \in \mathbb{Z})$

$cos\, x = a \Rightarrow x = \pm arccos\, a + 2k\pi \quad (k \in \mathbb{Z})$

$tan\, x = a \Rightarrow x = arctan\, a + k\pi \quad (k \in \mathbb{Z})$

$cot\, x = a \Rightarrow x = arc\, cot\, a + k\pi \quad (k \in \mathbb{Z})$

II. The equality of two trigonometric functions of the same name

$\sin u = \sin v \Rightarrow u = (-1)^k \cdot v + k\pi \quad (k \in \mathbb{Z})$

$\cos u = \cos v \Rightarrow u = \pm v + 2k\pi \quad (k \in \mathbb{Z})$

$\tan u = \tan v \Rightarrow u = v + k\pi \quad (k \in \mathbb{Z})$

$\cot u = \cot v \Rightarrow u = v + k\pi \quad (k \in \mathbb{Z})$

III. Trigonometric equations of the form $\sin f(x) = \sin g(x)$

$\sin f(x) = \sin g(x) \Rightarrow f(x) = (-1)^k g(x) + k\pi \quad (k \in \mathbb{Z})$

IV. Trigonometric equations reducible to equations which contain the same function of the same angle.

- The trigonometric equation is reduced to an algebraic equation in which the unknown is a trigonometric function of the angle which needs to be determined.

V. Homogeneous equations in $\sin x$ and $\cos x$

$a_0 \sin^n x + a_1 \sin^{n-1} x \cos x + a_2 \sin^{n-2} x \cos^2 x + \ldots + a_n \cos^n x = 0$

- We divide the equation by $\cos^n x$ and obtain an equation of n degree in $\tan x$:

$a_0 \tan^n x + a_1 \tan^{n-1} x + a_2 \tan^{n-2} x + \ldots + a_n = 0$

(Dividing by $\cos^n x$ there are no solutions lost).

VI. The linear equation in $\sin x$ and $\cos x$

1) The method of the auxiliary angle

$a \sin x + b \cos x = c \ | : a$

$\sin x + \frac{b}{a} \cos x = \frac{c}{a}$

Denote: $\sin x + \frac{b}{a} = \tan \varphi \quad -\frac{\pi}{2} < \varphi < +\frac{\pi}{2}$

$\sin x + \tan \varphi \cos x = \frac{c}{a}$

$\sin x \cos \varphi + \sin \varphi \cos x = \frac{c}{a} \cos \varphi$

$\sin(x + \varphi) = \frac{c}{a} \cos \varphi$

But $\cos \varphi = \frac{1}{\sqrt{1 + \tan^2 \varphi}} = \frac{|a|}{\sqrt{a^2 + b^2}}$

Therefore $\sin(x + \varphi) = \frac{c|a|}{a\sqrt{a^2 + b^2}} = \frac{c}{\pm\sqrt{a^2 + b^2}}$

We take the positive sign if $a > 0$ and the negative sign, when $a < 0$.

The equation has solutions if $\left| \frac{c}{\pm\sqrt{a^2 + b^2}} \right| \leq 1$, that is if $c^2 \leq a^2 + b^2$

$x = (-1)^k \arcsin \frac{c}{\pm\sqrt{a^2 + b^2}} + k\pi - \arctan \frac{b}{a} \quad (k \in \mathbb{Z})$

2) The substitution method

We substitute $sin\alpha = \frac{2t}{1+t^2}$; $cos\alpha = \frac{1-t^2}{1+t^2}$

$a\,sin x + b\,cos x = c$

$a\frac{2t}{1+t^2} + b\frac{1-t^2}{1+t^2} = c$

$(b+c)t^2 - 2at + (c-b) = 0$

Conditions: $c + b \neq 0$ and $\Delta \geq 0$

$\Delta = a^2 + b^2 - c^2 \geq 0 \Rightarrow c^2 \leq a^2 + b^2$

$\Delta = a^2 + b^2 - c^2 \geq 0 \Rightarrow c^2 \leq a^2 + b^2 \Rightarrow$

$\Rightarrow t = \frac{a \pm \sqrt{a^2 + b^2 - c^2}}{b+c} = tan\frac{\alpha}{2}$

$\Rightarrow x = 2\left(arctan\frac{a \pm \sqrt{a^2 + b^2 - c^2}}{b+c} + k\pi \right) \quad (k \in \mathbb{Z})$

Performing these substitutions we can lose solutions (values of angle x for which $tan\frac{x}{2}$ doesn't have sense: $\frac{\pi}{2} + k\pi \ (k \in \mathbb{Z})$, for this reason, after computation, we need to verify these values as well; if they verify, we add them to the set of solutions.

3) We can solve the system:

$$\begin{cases} a\,sin x + b\,cos x = c \\ sin^2 x + cos^2 x = 1 \end{cases}$$

We eliminate the foreign solution by verification, $sin\,x$ and $cos\,x$ are the unknown.

VII. Equation that can be resolved by decomposition in factors.

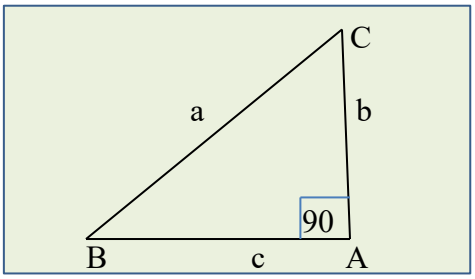
In some situations, the equations are resolved by appealing to the squaring process, but care has to be taken not to introduce foreign solutions.

Systems of trigonometric equations

- We do certain substitutions
- We decompose the products in sums or vice versa
- We use the fundamental trigonometric formulae.

Trigonometric applications in geometry

1. **Rectangle triangle**



$\sphericalangle B + \sphericalangle C = 90°$

$\sphericalangle A = 90°$

2. **Random triangle**

The sine theorem

$$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C} = 2R$$

The cosine theorem

$$a^2 = b^2 + c^2 - 2bc\cos A$$

The tangent theorem

$$\frac{a-b}{a+b} = \frac{\tan\frac{A-B}{2}}{\tan\frac{A+B}{2}}$$

The trigonometric functions of the angles of a triangle expressed using the sides of the triangle.

$$\sin\frac{A}{2} = \sqrt{\frac{(p-b)(p-c)}{bc}},\ldots$$

$$\cos\frac{A}{2} = \sqrt{\frac{p(p-a)}{bc}},\ldots$$

$$\tan\frac{A}{2} = \sqrt{\frac{(p-b)(p-c)}{p(p-a)}},\ldots$$

$$\cot\frac{A}{2} = \sqrt{\frac{p(p-a)}{(p-b)(p-c)}},\ldots$$

$$\cos A = \frac{a^2 + b^2 - c^2}{2bc}$$

Relations in a random triangle

$$R = \frac{abc}{4S}$$

S is the aria of the triangle

Euler's elation: $OI^2 = R(R-2r)$; O the center of the circumscribed circle, I is the center of the inscribed circle.

$$r = \frac{S}{p}$$

$$a = b \cdot \cos C + c \cdot \cos B, \ldots$$

$$r = 4R \sin\frac{A}{2}\sin\frac{B}{2}\sin\frac{C}{2} = p\tan\frac{A}{2}\tan\frac{B}{2}\tan\frac{C}{2} = \frac{S}{p} = \sqrt{\frac{(p-a)(p-b)(p-c)}{p}}$$

$$r_a = 4R \sin\frac{A}{2}\sin\frac{B}{2}\sin\frac{C}{2} = p\tan\frac{A}{2} = \frac{S}{p-a} = \sqrt{\frac{p(p-b)(p-c)}{(p-a)}}, \ldots$$

r_a is the radius of the triangle's ex-inscribed circle.

$$p = 4R\cos\frac{A}{2}\cos\frac{B}{2}\cos\frac{C}{2}$$

$$r_a + r_b + r_c = 4R + r$$

$$b_a = \frac{2bc}{b+c}\cos\frac{A}{2} = \frac{2R\sin B\sin C}{\cos\frac{B-C}{2}} = \frac{2\sqrt{bcp(p-a)}}{b+c}$$

$$b_a = \frac{c\sin B}{\cos\frac{B-C}{2}}, \ldots \ b_a \text{ is the bisector of } \sphericalangle A$$

$$m_a = \frac{1}{2}\sqrt{2(b^2+c^2)+a^2}, \ldots$$

$S = \sqrt{p(p-a)(p-b)(p-c)}$ - Heron's formula

$$S = \frac{abc\sin C}{2} = \frac{a^2\sin B\sin C}{2\sin(B+C)}, \ldots$$

Aria of a quadrilateral

$$S_{\square} = \frac{d_1 d_2 \sin\varphi}{2}$$ φ is the angle between the diagonals d_1, d_2

$$d_1 d_2 \le ac + bd$$

Trigonometric tables

To find the values of the trigonometric functions of various angles one uses the trigonometric tables, where these are listed.

Interpolation

Interpolation is an operation through which we can determine the trigonometric function's values of angles which cannot be found in the trigonometric tables.

Example:

$sin\,34°20' = 0.56401$

$sin\,34°30' = 0.56641$

How much is $sin\,34°22' = ?$

$sin\,34°20' < sin\,34°22' < sin\,34°30'$

$34°30' - 34°20'.....0.56641 - 0.56401$

$34°22' - 34°20'.....x$ $\Rightarrow sin\,34°22' = 0.56401 + 0.00048 = 0.56449$

$x = \dfrac{2 \cdot 0.00240}{10} = 0.00048$

Logarithmic tables of trigonometric functions

Example $ln\,sin\,17°34' = \bar{1}.47974$

Complex numbers under a trigonometric form

$i = \sqrt{-1}$

A complex number is a number of the format: $z = x + iy$, $x, y \in \mathbb{R}$

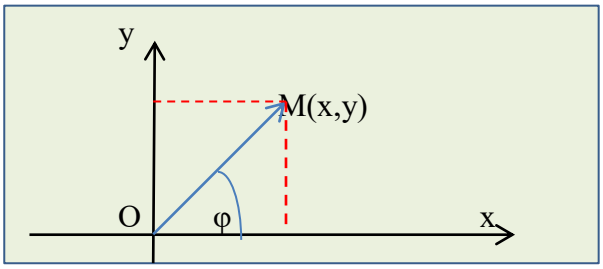
$i^{4m} = 1;\ i^{4m+1} = i;\ i^{4m+2} = -1;\ i^{4m+3} = -i$, $m \in \mathbb{Z}$

x is the real part

iy is the imaginary part

y is the coefficient of the imaginary part.

There is bi-univocal correspondence between the set of complex numbers $z = x + iy$ and the set of points $M(x, y)$ from plane.



The module of a complex number is the length of the segment OM, $|z|$

The argument of a complex number is the angle formed by the vector OM the x axis; $arg\,z$.

A complex plane is the plane in which we represent the complex numbers $z = x + iy$.

$|z| = \sqrt{x^2 + y^2}\ \ (= \rho)$

$tan\,\varphi = \dfrac{y}{x}$ or $sin\,\varphi = \dfrac{x}{\rho}; cos\,\varphi = \dfrac{y}{\rho}$

$z = \rho(cos\,\varphi + i\,sin\,\varphi)$.

The conjugate of the complex number $z = x + iy$ is the complex number $\bar{z} = x - iy$; $\bar{z} = |z|$; $arg\,\bar{z} = 2\pi - arg\,z$.

The sum and the difference of the complex numbers

Let $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$, then

$$z_1 + z_2 = x_1 + x_2 + i\left(y_1 + y_2\right)$$

$$\left(x_1 - x_2\right) + i\left(y_1 - y_2\right)$$

The multiplication of complex numbers

$$z_1 \cdot z_2 = \left(x_1 x_2 - y_1 y_2\right) + i\left(x_1 y_2 + x_2 y_1\right)$$

The multiplication is

- Commutative
- Associative
- Distributive relative to the sum of the complex numbers.

The module of the product of two complex numbers is equal to the product of their modules, and the product argument is equal to the sum of the arguments:

$$\left|z_1 \cdot z_2\right| = \left|z_1\right| \cdot \left|z_2\right|;$$

$$arg\left(z_1 \cdot z_2\right) = arg\, z_1 + arg\, z_2$$

$$z_1 = \rho_1\left(cos\,\varphi_1 + i\,sin\,\varphi_1\right)$$

$$z_2 = \rho_2\left(cos\,\varphi_2 + i\,sin\,\varphi_2\right)$$

$$z_1 \cdot z_2 = \rho_1\rho_2\left[cos\left(\varphi_1 + \varphi_2\right) + i\,sin\left(\varphi_1 + \varphi_2\right)\right]$$

Generalization:

$$z_1 \cdot z_2 ... z_n = \rho_1\rho_2 ... \rho_n\left[cos\left(\varphi_1 + \varphi_2 + ... + \varphi_n\right) + i\,sin\left(\varphi_1 + \varphi_2 + ... + \varphi_n\right)\right]$$

The division of the complex numbers

$$\left|\frac{z_1}{z_2}\right| = \frac{\left|z_1\right|}{\left|z_2\right|}$$

$$arg\left(\frac{z_1}{z_2}\right) = arg\, z_1 - arg\, z_2$$

$$\frac{z_1}{z_2} = -\frac{\rho_1}{\rho_2}\left[cos\left(\varphi_1 - \varphi_2\right) + i\,sin\left(\varphi_1 - \varphi_2\right)\right]$$

The power of the complex numbers (Moivre relation)

$$\left|z^n\right| = \left|z\right|^n$$

$$arg\left(z^n\right) = arg\left(nz\right)$$

$$z^n = \rho^n\left(cos\, n\varphi + i\,sin\, n\varphi\right)\ n \in \mathbb{Z}$$

The root of n order from a complex number

$$\left|\sqrt[n]{z}\right| = \left|z\right|^{\frac{1}{n}}$$

$$arg\sqrt[n]{z}=\frac{arg\,z+2k\pi}{n};k=0,1,2,...,n-1$$

$$\sqrt[n]{\rho\left(cos\,\varphi+i\,sin\,\varphi\right)}=\rho^{\frac{1}{n}}\left(cos\frac{\varphi+2k\pi}{n}+i\,sin\frac{\varphi+2k\pi}{n}\right);k=0,1,2,...,n-1$$

Binomial equations

A binomial equation is an equation of the form $z^n+\alpha=0$, where α is a complex number and z is the unknown $z\in\mathbb{R}$.

Example: Solve the following equation

$$\left(\frac{1+iz}{1-iz}\right)^4=\frac{\frac{1}{2}+\frac{\sqrt{3}}{2}i}{\frac{1}{2}-\frac{\sqrt{3}}{2}i}$$

$$\rho_1=\sqrt{\frac{1}{4}+\frac{3}{4}}=1$$

$$tan\,\varphi_1=\frac{\sqrt{3}}{2}\cdot\frac{2}{1}=\sqrt{3}\Rightarrow\varphi_1=\frac{\pi}{3}$$

$$z_1=\frac{1}{2}-\frac{\sqrt{3}}{2}i=cos\frac{\pi}{3}+i\,sin\frac{\pi}{3}$$

$$\varphi_2=\sqrt{\frac{1}{4}+\frac{3}{4}}=1$$

$$arg\,z_2=2\pi-arg\,z_1=2\pi-\frac{\pi}{3}=\frac{5\pi}{3}=\rho_2$$

$$\frac{z_1}{z_2}=cos\left(\frac{-4\pi}{3}\right)+i\,sin\left(\frac{-4\pi}{3}\right)=cos\frac{4\pi}{3}-i\,sin\frac{4\pi}{3}=cos\frac{2\pi}{3}+i\,sin\frac{2\pi}{3}$$

$$\frac{1+iz}{1-iz}=\sqrt[4]{cos\frac{2\pi}{3}+i\,sin\frac{2\pi}{3}}=cos\frac{\frac{2\pi}{3}+2k\pi}{4}+i\,sin\frac{\frac{2\pi}{3}+2k\pi}{4}$$

$$\frac{1+iz}{1-iz}=cos\,\alpha+i\,sin\,\alpha;\ \alpha=\left(\frac{2\pi}{3}+2k\pi\right)\cdot\frac{1}{4}$$

$$cos\,\alpha+i\,sin\,\alpha-iz\,cos\,\alpha-T-iz=0$$

$$z=\frac{cos\,\alpha+i\,sin\,\alpha-1}{i\left(cos\,\alpha+1\right)-sin\,\alpha}=\frac{-2\,sin^2\frac{\alpha}{2}+i-2\,sin\frac{\alpha}{2}cos\frac{\alpha}{2}}{-2\,sin\frac{\alpha}{2}cos\frac{\alpha}{2}+2\,cos^2\frac{\alpha}{2}}=$$

$$=\frac{2i\,sin\frac{\alpha}{2}\left(cos\frac{\alpha}{2}+i\,sin\frac{\alpha}{2}\right)}{2i\,cos\frac{\alpha}{2}\left(cos\frac{\alpha}{2}+i\,sin\frac{\alpha}{2}\right)}=tan\frac{\alpha}{2}$$

$$z = tan\frac{\frac{2\pi}{3} + 2k\pi}{2 \cdot 4} = tan\frac{\frac{\pi}{3} + k\pi}{4} \qquad k = 0,1,2,3$$

$$\begin{cases} k = 0 \Rightarrow z_1 = tan\dfrac{\pi}{12} \\ k = 1 \Rightarrow z_2 = tan\dfrac{\pi}{3} \\ k = 2 \Rightarrow z_3 = tan\dfrac{7\pi}{12} \\ k = 3 \Rightarrow z_4 = tan\dfrac{5\pi}{6} \end{cases}$$

Cebyshev polynomials

$T_n(x) = cos\, n\, arccos\, x$, where $n \in \mathbb{N}$, are polynomials of n degree, defined on $[-1,+1]$; these satisfy the relation:

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$$

$$arctan\frac{1}{2} + arctan\frac{1}{2 \cdot 2^2} + ... + arctan\frac{1}{2 \cdot 2^n} = arctan\frac{n}{n+1}$$

$$\frac{1 + tan\,\alpha}{1 - tan\,\alpha} = tan\left(\alpha + \frac{\pi}{4}\right)$$

- If $\alpha + \beta + \gamma = \pi$ then $sin\,\alpha + sin\,\beta + sin\,\gamma = 4\,cos\frac{\alpha}{2}cos\frac{\beta}{2}cos\frac{\gamma}{2}$
- If $\alpha + \beta + \gamma = \pi$ then $tan\,\alpha + tan\,\beta + tan\,\gamma = tan\,\alpha\, tan\,\beta\, tan\,\gamma$
- If $\alpha + \beta + \gamma = \pi$ and are positive, then $cos\,\alpha + cos\,\beta + cos\,\gamma = 1 + 4\,sin\frac{\alpha}{2}sin\frac{\beta}{2}sin\frac{\gamma}{2}$.

Sometimes the powers of the trigonometric fractions are transformed in linear equations. Example:

$sin^4 x = \left(sin^2 x\right)^2 = \left(\dfrac{1 - cos^2 x}{2}\right)^2$, etc.

$\left(sin\,x - cos\,x\right)^2 - 1 - sin\,2x$.

Sometimes we multiply both members of a relation with the same factor, but one has to make sure that foreign solutions are not introduced.

$\left(sin\,x - cos\,x\right)^2 - 1 - \frac{1}{2}sin^2 2x$

Chapter Six: Fields and Galois Theory

Abstract. This chapter develops some general theory for field extensions and then goes on to study Galois groups and their uses. More than half the chapter illustrates by example the power and usefulness of the theory of Galois groups. Prerequisite material from Chapter VIII consists of Sections 1–6 for Sections 1–13 of the present chapter, and it consists of all of Chapter VIII for Sections 14–17 of the present chapter.

Sections 1–2 introduce field extensions. These are inclusions of a base field in a larger field. The fundamental construction is of a simple extension, algebraic or transcendental, and the next construction is of a splitting field. An algebraic simple extension is made by adjoining a root of an irreducible polynomial over the base field, and a splitting field is made by adjoining all the roots of such a polynomial. For both constructions, there are existence and uniqueness theorems.

Section 3 classifies finite fields. For each integer q that is a power of some prime number, there exists one and only one finite field of order q, up to isomorphism. One finite field is an extension of another, apart from isomorphisms, if and only if the order of the first field is a power of the order of the second field.

Section 4 concerns algebraic closure. Any field has an algebraic extension in which each nonconstant polynomial over the extension field has a root. Such a field exists and is unique up to isomorphism.

Section 5 applies the theory of Sections 1–2 to the problem of constructibility with straightedge and compass. First the problem is translated into the language of field theory. Then it is shown that three desired constructions from antiquity are impossible: "doubling a cube," trisecting an arbitrary constructible angle, and "squaring a circle." The full proof of the impossibility of squaring a circle uses the fact that π is transcendental over the rationals, and the proof of this property of π is deferred to Section 14. Section 5 concludes with a statement of the theorem of Gauss identifying integers n such that a regular n-gon is constructible and with some preliminary steps toward its proof.

Sections 6–8 introduce Galois groups and develop their theory. The theory applies to a field extension with three properties—that it is finite-dimensional, separable, and normal. Such an extension is called a "finite Galois extension." The Fundamental Theorem of Galois Theory says in this case that the intermediate extensions are in one-one correspondence with subgroups of the Galois group, and it gives formulas relating the corresponding intermediate fields and Galois subgroups.

Sections 9–11 give three standard initial applications of Galois groups. The first is to proving the theorem of Gauss about constructibility of regular n-gons, the second is to deriving the Fundamental Theorem of Algebra from the Intermediate Value Theorem, and the third is to proving the necessity of the condition of Abel and Galois for solvability of polynomial equations by radicals—that the Galois group of the splitting field of the polynomial have a composition series with abelian quotients.

Sections 12–13 begin to derive quantitative information, rather than qualitative information, from Galois groups. Section 12 shows how an appropriate Galois group points to the specific steps in the construction of a regular n-gon when the construction is possible. Section 13 introduces a tool

known as Lagrange resolvents, a precursor of modern harmonic analysis. Lagrange resolvents are used first to show that Galois extensions in characteristic 0 with cyclic Galois group of prime order p are simple extensions obtained by adjoining a p^{th} root, provided all the p^{th} roots of 1 lie in the base field. Lagrange resolvents and this theorem about cyclic Galois groups combine to yield a derivation of Cardan's formula for solving general cubic equations.

Section 14 begins the part of the chapter that depends on results in the later sections of Chapter VIII. Section 14 itself contains a proof that π is transcendental; the proof is a nice illustration of the interplay of algebra and elementary real analysis.

Section 15 introduces the field polynomial of an element in a finite-dimensional extension field. The determinant and trace of this polynomial are called the norm and trace of the element. The section gives various formulas for the norm and trace, including formulas involving Galois groups. With these formulas in hand, the section concludes by completing the proof of Theorem 8.54 about extending Dedekind domains, part of the proof having been deferred from Section VIII.11.

Section 16 discusses how prime ideals split when one passes, for example, from the integers to the algebraic integers in a number field. The topic here was broached in the motivating examples for algebraic number theory and algebraic geometry as introduced in Section VIII.7, and it was the main topic of concern in that section. The present results put matters into a wider context.

Section 17 gives two tools that sometimes help in identifying Galois groups, particularly of splitting fields of monic polynomials with integer coefficients. One tool uses the discriminant of the polynomial. The other uses reduction of the coefficients modulo various primes.

1. Algebraic Elements

If $\mathbb{K}$ and $\Bbbk$ are fields such that $\Bbbk$ is a subfield of $\mathbb{K}$, we say that $\mathbb{K}$ is a **field extension** of $\Bbbk$. When it is necessary to refer to this situation in some piece of notation, we often write $\mathbb{K}/\Bbbk$ to indicate the field extension. In this section we shall study field extensions in a general way, and in the next section we shall discuss constructions and uniqueness results involving them.

If $\mathbb{K}$ and $\mathbb{K}'$ are two fields and if φ is a ring homomorphism of $\mathbb{K}$ into $\mathbb{K}'$ with $\varphi(1) = 1$, then φ is automatically one-one since $\mathbb{K}$ has no nontrivial ideals. We refer to φ as a **field map** or **field mapping**.[1] If $\mathbb{K}$ and $\mathbb{K}'$ are both field extensions of a field $\Bbbk$ and if the restriction of a field map φ to $\Bbbk$ is the identity, then φ is called a $\Bbbk$ **field map** or a **field map fixing** $\Bbbk$. The terminology "$\Bbbk$ field map" is consistent with the view that $\mathbb{K}$ and $\mathbb{K}'$ are two R algebras for $R = \Bbbk$ in the sense of Examples 6 and 15 in Section VIII.1, and that the isomorphism in question is just an R algebra isomorphism.

If a field map $\varphi : \mathbb{K} \to \mathbb{K}'$ is onto $\mathbb{K}'$, then φ is a **field isomorphism**; it is a $\Bbbk$ **field isomorphism** if $\mathbb{K}$ and $\mathbb{K}'$ are extensions of $\Bbbk$ and φ is the identity on $\Bbbk$. When $\mathbb{K} = \mathbb{K}'$ and φ is onto $\mathbb{K}'$, φ is called an **automorphism** of $\mathbb{K}$; if also φ is the identity on a subfield $\Bbbk$, then φ is called a $\Bbbk$ **automorphism** of $\mathbb{K}$.

[1] This is the notion of morphism in the category of fields.

Pure Mathematical Physics

Throughout this section we let $\mathbb{K}/\Bbbk$ be a field extension. If $x_1, \dots, x_n$ are members of $\mathbb{K}$, we let

$$\Bbbk[x_1, \dots, x_n] = \text{subring of } \mathbb{K} \text{ generated by 1 and } x_1, \dots, x_n,$$

$$\Bbbk(x_1, \dots, x_n) = \text{subfield of } \mathbb{K} \text{ generated by 1 and } x_1, \dots, x_n.$$

The latter, in more detail, means the set of all quotients ab^{-1} with a and b in $\Bbbk[x_1, \dots, x_n]$ and with $b \neq 0$. It is referred to as the **field obtained by adjoining** $x_1, \dots, x_n$ to $\Bbbk$. Because of this description of the elements of $\Bbbk(x_1, \dots, x_n)$, the field $\Bbbk(x_1, \dots, x_n)$ can be regarded as the field of fractions $\mathbb{F}$ of $\Bbbk[x_1, \dots, x_n]$. In fact, we argue as follows: let $\eta : \Bbbk[x_1, \dots, x_n] \to \mathbb{F}$ be the natural ring homomorphism $a \mapsto$ class of $(a, 1)$ of $\Bbbk[x_1, \dots, x_n]$ into its field of fractions; then the universal mapping property of $\mathbb{F}$ stated in Proposition 8.6 gives a factorization of the inclusion $\iota : \Bbbk[x_1, \dots, x_n] \to \Bbbk(x_1, \dots, x_n)$ as $\iota = \widetilde{\iota}\eta$, and the field mapping $\widetilde{\iota}$ has to be onto $\Bbbk(x_1, \dots, x_n)$ since the class of (a, b) maps to the member ab^{-1} of $\Bbbk(x_1, \dots, x_n)$.

As in Chapter IV and elsewhere, we let $\Bbbk[X]$ be the ring of polynomials in the indeterminate X with coefficients in $\Bbbk$. For each x in $\mathbb{K}$, we have a unique substitution homomorphism $\varphi_x : \Bbbk[X] \to \Bbbk[x]$ carrying $\Bbbk$ to itself and carrying X to x. We say that x is **algebraic** over $\Bbbk$ if φ_x is not one-one, i.e., if x is a root of some nonzero polynomial in $\Bbbk[X]$, and that x is **transcendental** over $\Bbbk$ if φ_x is one-one.

EXAMPLES.

(1) If $\Bbbk = \mathbb{R}$, if $\mathbb{K} = \mathbb{C}$, and if x is the usual element $i = \sqrt{-1}$, then $\varphi_i(X^2 + 1) = 0$, and i is algebraic over $\mathbb{R}$.

(2) If $\Bbbk = \mathbb{Q}$, if $\mathbb{K} = \mathbb{C}$, and if θ is a complex number with the property that $\theta^n + c_{n-1}\theta^{n-1} + \cdots + c_1\theta + c_0 = 0$ for some n and for some coefficients in $\mathbb{Q}$, then θ is algebraic over $\mathbb{Q}$. This situation was the subject of Proposition 4.1, of Example 2 in Section IV.4, and of Example 10 in Section VIII.1.

(3) Let $\Bbbk = \mathbb{Q}$ and $\mathbb{K} = \mathbb{C}$. For π equal to the usual trigonometric constant, given as the least positive real such that $e^{i\pi} = -1$ when $e^z = \sum_{n=0}^{\infty} z^n/n!$, it will be proved in Section 14 that there is no polynomial $F(X)$ in $\mathbb{Q}[X]$ with $F(\pi) = 0$, and π is consequently transcendental over $\mathbb{Q}$.

(4) If $\Bbbk = \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{K}$ is the 4-element field constructed in Example 3 of fields in Section IV.4, then any element of $\mathbb{K}$ is algebraic over $\Bbbk$.

(5) If $\Bbbk = \mathbb{C}(X)$ and if $\mathbb{K} = \mathbb{C}(X)[\sqrt{(X-1)X(X+1)}\,]$ as with the ring R' in Section VIII.7 and as in Example 3 of integral closures in Section VIII.9, then $\sqrt{(X-1)X(X+1)}$ is algebraic over $\mathbb{C}(X)$.

Pure Mathematical Physics

Suppose that x in $\mathbb{K}$ is algebraic over $\Bbbk$. Then

$$\ker \varphi_x = \{F(X) \in \Bbbk[X] \mid F(x) = 0\}$$

is an ideal in $\Bbbk[X]$ that is necessarily nonzero and principal. A generator is determined up to a constant factor as any nonzero polynomial in the ideal that has lowest possible degree, and we might as well take this polynomial to be monic. Thus $\ker \varphi_x$ is of the form $(F_0(X))$ for some unique monic polynomial $F_0(X)$, and this polynomial $F_0(X)$ is called the **minimal polynomial** of x over $\Bbbk$. Review of the example at the end of Section VIII.3 may help motivate the first five results below.

Proposition 9.1 If $x \in \mathbb{K}$ is algebraic over $\Bbbk$, then the minimal polynomial of x over $\Bbbk$ is prime as a polynomial in $\mathbb{K}[X]$.

PROOF. Suppose that $F(X)$ factors nontrivially as $F(X) = G(X)H(X)$. Since $F(x) = 0$, either $G(x) = 0$ or $H(x) = 0$, and then we have a contradiction to the fact that F has minimal degree among all polynomials vanishing at x. □

Theorem 9.2. If $x \in \mathbb{K}$ is algebraic over $\Bbbk$, then the field $\Bbbk(x)$ coincides with the ring $\Bbbk[x]$. Moreover, if the minimal polynomial of x over $\Bbbk$ has degree n, then each element of $\Bbbk(x)$ has a unique expansion as

$$c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1 x + c_0 \qquad \text{with all } c_i \in \Bbbk.$$

PROOF. Since the substitution ring homomorphism φ_x carries $\Bbbk[X]$ onto $\Bbbk[x]$, we have an isomorphism of rings $\Bbbk[x] \cong \Bbbk[X]/\ker \varphi_x = \Bbbk[X]/(F_0(X))$, where $F_0(X)$ is the minimal polynomial of x over $\Bbbk$. Since F_0 is prime, $(F_0(X))$ is a nonzero prime ideal and hence is maximal. Thus $\Bbbk[x]$ is a field. Consequently $\Bbbk(x) = \Bbbk[x]$.

Any element in $\Bbbk[x]$, hence in $\Bbbk(x)$, is a polynomial in x. Since $F_0(x) = 0$, we can solve $F_0(x) = 0$ for its leading term, say x^n, obtaining $x^n = G(x)$, where $G(X) = 0$ or $\deg G(X) \le n - 1$. Thus the expansions in the statement of the theorem yield all the members of $\Bbbk[x]$. If an element has two such expansions, we subtract them and obtain a nonzero polynomial $H(X)$ of degree at most $n - 1$ with $H(x) = 0$, in contradiction to the minimality of the degree of $F_0(X)$. □

Corollary 9.3. If $x \in \mathbb{K}$ is algebraic over $\Bbbk$, then the field $\Bbbk(x)$, regarded as a vector space over $\Bbbk$, is of dimension n, where n is the degree of the minimal polynomial of x over $\Bbbk$. The elements $1, x, x^2, \ldots, x^{n-1}$ form a basis of $\Bbbk(x)$ over $\Bbbk$.

PROOF. This is just a restatement of the second conclusion of Theorem 9.2. □

Pure Mathematical Physics

We say that the field extension $\mathbb{K}/\Bbbk$ is an **algebraic extension** if every element of $\mathbb{K}$ is algebraic over $\Bbbk$.

Proposition 9.4. If the vector-space dimension of $\mathbb{K}$ over $\Bbbk$ is some finite n, then $\mathbb{K}$ is an algebraic extension of $\Bbbk$, and each element x of $\mathbb{K}$ has some nonzero polynomial $F(X)$ in $\Bbbk[X]$ of degree at most n for which $F(x) = 0$.

PROOF. This is immediate since the elements $1, x, x^2, \dots, x^n$ of $\mathbb{K}$ have to be linearly dependent over $\Bbbk$. □

When $\mathbb{K}/\Bbbk$ is a field extension, we write $[\mathbb{K} : k]$ for the vector-space dimension $\dim_{\Bbbk} \mathbb{K}$, and we call this the **degree** of $\mathbb{K}$ over $\Bbbk$. If $[\mathbb{K} : \Bbbk]$ is finite, we say that $\mathbb{K}$ is a **finite extension** of $\Bbbk$, or **finite algebraic extension** of $\Bbbk$, the condition "algebraic" being automatic by Proposition 9.4.

Corollary 9.5. If x is in $\mathbb{K}$, then x is algebraic over $\Bbbk$ if and only if $\Bbbk(x)$ is a finite algebraic extension of $\Bbbk$. In this case the minimal polynomial of x over $\Bbbk$ has degree $[\Bbbk(x) : \Bbbk]$.

PROOF. If x is algebraic over $\Bbbk$, then $[\Bbbk(x) : \Bbbk]$ is finite and is the degree of the minimal polynomial of x over $\Bbbk$, by Corollary 9.3. Proposition 9.4 shows in this case that $\Bbbk(x)$ is a finite algebraic extension. If x is transcendental over $\Bbbk$, then the substitution homomorphism φ_x is one-one, and $\dim_{\Bbbk} \Bbbk(x) \geq \dim_{\Bbbk} \Bbbk[X] = +\infty$. □

Theorem 9.6. Let $\Bbbk$, $\mathbb{K}$, and $\mathbb{L}$ be fields with $\Bbbk \subseteq \mathbb{K} \subseteq \mathbb{L}$, and suppose that $[\mathbb{K} : \Bbbk] = n$ and $[\mathbb{L} : \mathbb{K}] = m$, finite or infinite. Let $\{\omega_1, \omega_2, \dots\}$ be a vector-space basis of $\mathbb{K}$ over $\Bbbk$, and let $\{\xi_1, \xi_2, \dots\}$ be a vector-space basis of $\mathbb{L}/\mathbb{K}$. Then the mn products $\omega_i \xi_j$ form a basis of $\mathbb{L}$ over $\Bbbk$.

PROOF OF SPANNING. If ξ is in $\mathbb{L}$, write $\xi = \sum_j a_j \xi_j$ with each a_j in $\mathbb{K}$ and with only finitely many a_j's not 0. Then expand each a_j in terms of the ω_i's, and substitute. □

PROOF OF LINEAR INDEPENDENCE. Let $\sum_{i,j} c_{ij} \omega_i \xi_j = 0$ with the c_{ij}'s in $\Bbbk$. Since the members ξ_j of $\mathbb{L}$ are linearly independent over $\mathbb{K}$, $\sum_i c_{ij} \omega_i = 0$ for each j. Since the members ω_i of $\mathbb{K}$ are linearly independent over $\Bbbk$, $c_{ij} = 0$ for all i and j. □

Corollary 9.7. If $\Bbbk$, $\mathbb{K}$, and $\mathbb{L}$ are fields with $\Bbbk \subseteq \mathbb{K} \subseteq \mathbb{L}$, then

$$\boxed{[\mathbb{L} : \Bbbk] = [\mathbb{L} : \mathbb{K}]\,[\mathbb{K} : \Bbbk]\,.}$$

PROOF. This is immediate by counting basis elements in Theorem 9.6.

Pure Mathematical Physics

Theorem 9.8. If $\mathbb{K}/\Bbbk$ is a field extension and if $x_1, \ldots, x_n$ are members of $\mathbb{K}$ that are algebraic over $\Bbbk$, then $\Bbbk(x_1, \ldots, x_n)$ is a finite algebraic extension of $\Bbbk$.

REMARK. If a finite algebraic extension of $\Bbbk$ turns out to be of the form $\Bbbk(x)$ for some x, we say that the extension is a **simple algebraic extension**.

PROOF. Since x_i is algebraic over $\Bbbk$, it is algebraic over $\Bbbk(x_1, \ldots, x_{i-1})$. Hence $[\Bbbk(x_1, \ldots, x_i) : \Bbbk(x_1, \ldots, x_{i-1})]$ is finite. Applying Corollary 9.7 repeatedly, we see that $\Bbbk(x_1, \ldots, x_n)$ is a finite extension of $\Bbbk$. Proposition 9.4 shows that it is a finite algebraic extension. □

EXAMPLE. The sum $\sqrt{2}+\sqrt[3]{2}$ is algebraic over $\mathbb{Q}$, as a consequence of Theorem 9.8. This fact suggests Corollary 9.9 below.

Corollary 9.9 If $\mathbb{K}/\Bbbk$ is a field extension, then the elements of $\mathbb{K}$ that are algebraic over $\Bbbk$ form a field.

PROOF. If x and y in $\mathbb{K}$ are algebraic over $\Bbbk$, then $\Bbbk(x, y)$ is a finite algebraic extension of $\Bbbk$, according to Theorem 9.8. This extension contains $x \pm y$ and xy, and it contains x^{-1} if $x \neq 0$. The corollary therefore follows from Proposition 9.4. □

For the special case of Corollary 9.9 in which $\mathbb{K} = \mathbb{C}$ and $\Bbbk = \mathbb{Q}$, this subfield of $\mathbb{C}$ is called the field of **algebraic numbers**, and any finite algebraic extension of $\mathbb{Q}$ within $\mathbb{C}$ is called a **number field**, or an **algebraic number field**. The seeming discrepancy between this definition and the definition given in remarks with Proposition 4.1 (that in essence a "number field" is any simple algebraic extension of $\mathbb{Q}$) will be resolved by the Theorem of the Primitive Element (Theorem 9.34 below).

2. Construction of Field Extensions

In this section, $\Bbbk$ denotes any field. Our interest will be in constructing extension fields for $\Bbbk$ and in addressing the question of uniqueness under additional hypotheses. We begin with a kind of converse to Proposition 9.1 that generalizes the method described in Section A4 of the appendix for constructing $\mathbb{C} = \mathbb{R}(\sqrt{-1}\,)$ from $\mathbb{R}$ and the polynomial $X^2 + 1$.

Theorem 9.10 (existence theorem for simple algebraic extensions). If $F(X)$ is a monic prime polynomial in $\Bbbk[X]$, then there exists a simple algebraic extension $\mathbb{K} = \Bbbk(x)$ of $\Bbbk$ such that x is a root of $F(X)$. Moreover, $F(X)$ is the minimal polynomial of x over $\Bbbk$.

PROOF. Define $\mathbb{K} = \Bbbk[X]/(F(X))$ as a ring. Since $F(X)$ is prime, $(F(X))$ is a nonzero prime ideal, hence maximal. Therefore $\mathbb{K}$ is a field, an extension field of $\Bbbk$. Define x to be the coset $X + (F(X))$. Then $F(x) = F(X) + (F(X)) = 0 + (F(X))$, and x is therefore algebraic over $\Bbbk$. It is immediate that $\mathbb{K} = \Bbbk[x]$, and Theorem 9.2 shows that $\mathbb{K} = \Bbbk(x)$. If $G(x) = 0$ for some $G(X)$ in $\Bbbk[X]$, then $G(X)$ is in $(F(X))$. We conclude that $F(X)$ has minimal degree among all polynomials with x as a root, and $F(X)$ is therefore the minimal polynomial. □

Theorem 9.11 (uniqueness theorem for simple algebraic extensions). If $F(X)$ is a monic prime polynomial in $\Bbbk[X]$ and if $\mathbb{K} = \Bbbk(x)$ and $\mathbb{K}' = \Bbbk(y)$ are two simple algebraic extensions such that x and y are roots of $F(X)$, then there exists a field isomorphism φ of $\mathbb{K}$ onto $\mathbb{K}'$ fixing $\Bbbk$ and carrying x to y.

EXAMPLE. The monic polynomial $F(X) = X^3 - 2$ is prime in $\mathbb{Q}[X]$, and $x = \sqrt[3]{2}$ and $y = e^{2\pi i/3}\sqrt[3]{2}$ are roots of it within $\mathbb{C}$. The fields $\mathbb{Q}(x)$ and $\mathbb{Q}(y)$ are subfields of $\mathbb{C}$ and are distinct because $\mathbb{Q}(x)$ is contained in $\mathbb{R}$ and $\mathbb{Q}(y)$ is not. Nevertheless, these fields are $\mathbb{Q}$ isomorphic, according to the theorem.

PROOF. In view of the proof of Theorem 9.10, there is no loss of generality in assuming that $\mathbb{K} = \Bbbk[X]/(F(X))$. Since y is algebraic over $\Bbbk$, we can form the substitution homomorphism $\varphi_y : \Bbbk[X] \to \Bbbk(y)$. This is a $\Bbbk$ algebra homomorphism. Its kernel is the ideal $(F(X))$ since $F(X)$ is the minimal polynomial of y, and φ_y therefore descends to a one-one $\Bbbk$ algebra homomorphism $\overline{\varphi_y} : \Bbbk(x) \to \Bbbk(y)$. Since $\dim \Bbbk(x)$ and $\dim \Bbbk(y)$ both match the degree of $F(X)$, $\overline{\varphi_y}$ is onto $\Bbbk(y)$ and is therefore the required $\Bbbk$ isomorphism. □

We say that a nonconstant polynomial $F(X)$ in $\Bbbk[X]$ **splits** in a given extension field if $F(X)$ factors completely into degree-one factors over that extension field. A **splitting field** over $\Bbbk$ for a nonconstant polynomial $F(X)$ in $\Bbbk[X]$ is an extension field $\mathbb{L}$ of $\Bbbk$ such that $F(X)$ splits in $\mathbb{L}$ and such that $\mathbb{L}$ is generated by $\Bbbk$ and the roots of $F(X)$ in $\mathbb{L}$.

EXAMPLES. Let $\Bbbk = \mathbb{Q}$. Then $\mathbb{Q}(\sqrt{-1}\,)$ is a splitting field for $X^2 + 1$, because $\pm\sqrt{-1}$ are both in $\mathbb{Q}(\sqrt{-1}\,)$ and they generate $\mathbb{Q}(\sqrt{-1}\,)$ over $\mathbb{Q}$. But $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field for $X^3 - 2$ because $\mathbb{Q}(\sqrt[3]{2})$ does not contain the two nonreal roots of $X^3 - 2$.

Theorem 9.12 (existence of splitting field). If $F(X)$ is a nonconstant polynomial in $\Bbbk[X]$, then there exists a splitting field of $F(X)$ over $\Bbbk$.

PROOF. We begin by constructing a certain extension field $\mathbb{K}$ of $\Bbbk$ in which $F(X)$ factors completely into degree-one factors in $\mathbb{K}[X]$. We do so by induction on $n = \deg F(X)$. For $n = 1$, there is nothing to prove. For general n, let $G(X)$

Pure Mathematical Physics

be a prime factor of $F(X)$, and apply Theorem 9.10 to obtain a simple algebraic extension $\Bbbk_1 = \Bbbk(x_1)$ over $\Bbbk$ such that $G(x_1) = 0$. Then $F(x_1) = 0$, and the Factor Theorem (Corollary 1.13) gives $F(X) = (X - x_1)H(X)$ for some $H(X)$ in $\Bbbk_1(X)$ of degree $n - 1$. Since $\deg H(X) = n - 1 < \deg F(X)$, the inductive hypothesis produces an extension $\mathbb{K}$ of $\Bbbk_1$ such that $H(X)$ is a constant multiple of $(X - x_2) \cdots (X - x_n)$ with all x_i in $\mathbb{K}$. Then $F(X)$ factors into degree-one factors in $\mathbb{K}[X]$, and the induction is complete.

Within the constructed field $\mathbb{K}$, let $\mathbb{L}$ be the subfield $\mathbb{L} = \Bbbk(x_1, \ldots, x_n)$. Then $F(X)$ still factors completely into degree-one factors in $\mathbb{L}(X)$, and $\mathbb{L}$ is generated by $\Bbbk$ and the x_i. Hence $\mathbb{L}$ is a splitting field.

EXAMPLES OF SPLITTING FIELDS.

(1) $\Bbbk = \mathbb{Q}$ and $F(X) = X^3 - 2$. The proof of Theorem 9.12 takes $\Bbbk_1 = \mathbb{Q}(\sqrt[3]{2})$ and writes $X^3 - 2 = (X - \sqrt[3]{2})\big(X^2 + \sqrt[3]{2}\,X + (\sqrt[3]{2})^2\big)$. Then the proof adjoins one root θ (hence both roots) of $X^2 + \sqrt[3]{2}\,X + (\sqrt[3]{2})^2$, setting $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, \theta)$. With this choice of $\mathbb{K}$, the splitting field turns out to be $\mathbb{L} = \mathbb{K}$. In fact, to see that $\mathbb{L}$ is not a proper subfield of $\mathbb{K}$, we observe that $6 = [\mathbb{K} : \Bbbk] = [\mathbb{K} : \mathbb{L}]\,[\mathbb{L} : \mathbb{Q}]$ by Corollary 9.7 and that the proper containment $\mathbb{L} \supsetneq \mathbb{Q}(\sqrt[3]{2})$ implies $[\mathbb{L} : \mathbb{Q}] > 3$. Since $[\mathbb{L} : \mathbb{Q}]$ is a divisor of 6 greater than 3, $[\mathbb{L} : \mathbb{Q}] = 6$. Thus $[\mathbb{K} : \mathbb{L}] = 1$, and $\mathbb{K} = \mathbb{L}$.

(2) $\Bbbk = \mathbb{Q}$ and $F(X) = X^3 - X - \frac{1}{3}$. Application of Corollary 8.20c to the polynomial $G(X) = -3X^2F(1/X) = X^3 + 3X^2 - 3$ shows that $G(X)$ has no degree-one factor and hence is irreducible over $\mathbb{Q}$. Then it follows that $F(X)$ is irreducible over $\mathbb{Q}$. The proof of Theorem 9.12 takes $\Bbbk_1 = \mathbb{Q}(r)$, where $r^3 - r - \frac{1}{3} = 0$. Then division gives

$$X^3 - X - \tfrac{1}{3} = (X - r)(X^2 + rX + (r^2 - 1)).$$

The discriminant $b^2 - 4ac$ of the quadratic factor is

$$r^2 - 4(r^2 - 1) = 4 - 3r^2 = \frac{r^2}{(1 + 2r)^2},$$

the right-hand equality following from direct computation. This discriminant is a square in $\Bbbk_1 = \mathbb{Q}(r)$, and hence $X^2 + rX + (r^2 - 1)$ factors into degree-one factors in $\mathbb{Q}(r)$ without passing to an extension field. Therefore $\mathbb{L} = \mathbb{Q}(r)$ with $[\mathbb{L} : \mathbb{Q}] = 3$.

Theorem 9.13 (uniqueness of splitting field). If $F(X)$ is a nonconstant polynomial in $\Bbbk[X]$, then any two splitting fields of $F(X)$ over $\Bbbk$ are $\Bbbk$ isomorphic.

Pure Mathematical Physics

The idea of the proof is simple enough, but carrying out the idea runs into a technical complication. The idea is to proceed by induction, using the uniqueness result for simple algebraic extensions (Theorem 9.11) repeatedly until all the roots have been addressed. The difficulty is that after one step the coefficients of the two quotient polynomials end up in two distinct but $\Bbbk$ isomorphic fields. Thus at the second step Theorem 9.11 does not apply directly. What is needed is the reformulated version given below as Theorem 9.11′, which lends itself to this kind of induction. In addition, as soon as the induction involves at least three steps, the above statement of Theorem 9.13 does not lend itself to a direct inductive proof. For this reason we shall instead prove a reformulated version Theorem 9.13′ of Theorem 9.13 that is ostensibly more general than Theorem 9.13.

Recall from Proposition 4.24 that a general substitution homomorphism that starts from a polynomial ring can have two ingredients. One is the substitution of some element, such as x, for the indeterminate X, and the other is a homomorphism that is made to act on the coefficients. If the homomorphism is σ, let us write $F^\sigma(X)$ to indicate the polynomial obtained by applying σ to each coefficient of $F(X)$.

Theorem 9.11′. Let $\Bbbk$ and $\Bbbk'$ be fields, and let $\sigma : \Bbbk \to \Bbbk'$ be a field isomorphism. Suppose that $F(X)$ is a monic prime polynomial in $\Bbbk[X]$ and that $\mathbb{K} = \Bbbk(x)$ and $\mathbb{K}' = \Bbbk'(x')$ are simple algebraic extensions such that $F(x) = 0$ and $F^\sigma(x') = 0$. Then there exists a field isomorphism $\varphi : \Bbbk(x) \to \Bbbk'(x')$ such that $\varphi\big|_{\Bbbk} = \sigma$ and $\varphi(x) = x'$.

PROOF. The argument is essentially unchanged from the proof of Theorem 9.11. We start from the substitution homomorphism $G(X) \mapsto G^\sigma(x')$ that replaces X by x' and that operates by σ on the coefficients. This descends to a field map of $\Bbbk[x]$ into $\Bbbk'[x']$, and the homomorphism must be onto $\Bbbk'[x']$ by a count of dimensions. □

Theorem 9.13′. Let $\Bbbk$ and $\Bbbk'$ be fields, and let $\sigma : \Bbbk \to \Bbbk'$ be a field isomorphism. If $F(X)$ is a nonconstant polynomial in $\Bbbk[X]$ and if $\mathbb{L}$ and $\mathbb{L}'$ are respective splitting fields for $F(X)$ over $\Bbbk$ and for $F^\sigma(X)$ over $\Bbbk'$, then there exists a field isomorphism $\varphi : \mathbb{L} \to \mathbb{L}'$ such that $\varphi\big|_{\Bbbk} = \sigma$ and such that φ sends the set of roots of $F(X)$ to the set of roots of $F^\sigma(X)$.

PROOF. We proceed by induction on $n = \deg F(X)$, the case $n = 1$ being evident. Assume the result for degree $n-1$. Let $G(X)$ be a prime factor of $F(X)$ over $\Bbbk$. Then $G^\sigma(X)$ is a prime factor of $F^\sigma(X)$ over $\Bbbk'$. The polynomials $G(X)$ and $G^\sigma(X)$ have roots in $\mathbb{L}$ and $\mathbb{L}'$, respectively. Fix one such root for each, say x_1 and x_1'. By Theorem 9.11′, there exists a field isomorphism $\sigma_1 : \Bbbk(x_1) \to \Bbbk'(x_1')$ extending σ and satisfying $\sigma_1(x_1) = x_1'$. Write $F(X) = (X - x_1)H(X)$ with coefficients in $\Bbbk(x_1)$, by the Factor Theorem (Corollary 1.13). Applying σ_1 to

the coefficients, we obtain $F^\sigma(X) = (X - x_1')H^{\sigma_1}(X)$ with coefficients in $\Bbbk'(x_1')$. Then $\mathbb{L}$ and $\mathbb{L}'$ are splitting fields for $H(X)$ and $H^{\sigma_1}(X)$ over $\Bbbk(x_1)$ and $\Bbbk'(x_1')$, respectively. By induction we can extend σ_1 to an isomorphism $\varphi : \mathbb{L} \to \mathbb{L}'$, and the theorem readily follows. □

3. Finite Fields

In this section we shall use the results on splitting fields in Section 2 to classify finite fields up to isomorphism. So far, the examples of finite fields that we have encountered are the prime fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with p elements, p being any prime number, and the field of 4 elements in Example 3 of fields in Section IV.4. Every finite field has to contain a subfield isomorphic to one of the prime fields $\mathbb{F}_p$, and Proposition 4.33 observed as a consequence that any finite field necessarily has p^n elements for some prime number p and some integer $n > 0$.

Theorem 9.14. For each p^n with p a prime number and with n a positive integer, there exists up to isomorphism one and only one field with p^n elements. Such a field is a splitting field for $X^{p^n} - X$ over the prime field $\mathbb{F}_p$.

If $q = p^n$, it is customary to denote by $\mathbb{F}_q$ a field of order q. The theorem says that $\mathbb{F}_q$ exists and is unique up to isomorphism. Some authors refer to finite fields as **Galois fields**.

Some preparation is needed before we can come to the proof of the theorem. We need to carry over the simplest aspects of differential calculus to polynomials with coefficients in an arbitrary field $\Bbbk$. First we give an informal definition of the **derivative** of a polynomial; then we give a more precise definition. For any polynomial $F(X) = \sum_{j=0}^n c_j X^j$ in $\Bbbk[X]$, we informally define the derivative to be the polynomial

$$F'(X) = \sum_{j=1}^{n} j c_j X^{j-1} = \sum_{j=0}^{n-1} (j+1) c_{j+1} X^j.$$

The more precise definition uses the definition of members of $\Bbbk[X]$ as infinite sequences of members of $\Bbbk$ whose terms are 0 from some point on. In this notation if $F = (c_0, c_1, \dots, c_n, 0, \dots)$ with c_j in the j^{th} position for $j \le n$ and with 0 in the j^{th} position for $j > n$, then $F' = (c_1, 2c_2, \dots, nc_n, 0, \dots)$ with $(j+1)c_{j+1}$ in the j^{th} position for $j \le n-1$ and with 0 in the j^{th} position for $j > n-1$. In any event, the mapping $F \mapsto F'$ is $\Bbbk$ linear from $\Bbbk[X]$ to itself. The operation is called **differentiation**.

Proposition 9.15. Differentiation on $\mathbb{k}[X]$ satisfies the product rule: $F = GH$ implies $F' = G'H + GH'$.

PROOF. Because of the $\mathbb{k}$ linearity, it is enough to prove the result for monomials. Thus let $G(X) = X^m$ and $H(X) = X^n$, so that $F(X) = X^{m+n}$. Then $F'(X) = (m+n)X^{m+n-1}$, $G'(X)H(X) = mX^{m+n-1}$, and $G(X)H'(X) = nX^{m+n-1}$. Hence we indeed have $F'(X) = G'(X)H(X) + G(X)H'(X)$. □

Corollary 9.16. If n is a positive integer, if r is in $\mathbb{k}$, and if $F(X) = (X-r)^n$ in $\mathbb{k}[X]$, then $F'(X) = n(X-r)^{n-1}$.

PROOF. This is immediate by induction from Proposition 9.15 since the derivative of $X - r$ is 1. □

Corollary 9.17. Let r be in $\mathbb{k}$, and let $F(X)$ be in $\mathbb{k}[X]$. If $(X-r)^2$ divides $F(X)$, then $F(r) = F'(r) = 0$. Conversely if $F(r) = F'(r) = 0$, then $(X-r)^2$ divides $F(X)$.

PROOF. Write $F(X) = (X-r)^2G(X)$. If we substitute r for X, we see that $F(r) = 0$. If instead we differentiate, using Proposition 9.15 and Corollary 9.16, then we obtain $F'(X) = 2(X-r)G(X) + (X-r)^2G'(X)$. Substituting r for X, we obtain $F'(r) = 0 + 0 = 0$.

For the converse, let $F(r) = F'(r) = 0$. Proposition 4.28a shows that $F(X) = (X-r)G(X)$. Differentiating this identity by means of Proposition 9.15 gives $F'(X) = G(X) + (X-r)G'(X)$. Substituting r for X yields $0 = F'(r) = G(r) + 0$ and shows that $G(r) = 0$. By Proposition 4.28, $G(X) = (X-r)H(X)$. Hence $F(X) = (X-r)^2H(X)$. □

Lemma 9.18. If $\mathbb{k}$ is a field of characteristic $p \neq 0$, then the map $\varphi : \mathbb{k} \to \mathbb{k}$ given by $\varphi(x) = x^p$ is a field mapping.

REMARK. The map $x \mapsto x^p$ is often called the **Frobenius** map. If $\mathbb{k}$ is a finite field, then it must carry $\mathbb{k}$ onto $\mathbb{k}$ since one-one implies onto for functions from a finite set to itself; in this case the map is an automorphism of $\mathbb{k}$.

PROOF. The computation $\varphi(uv) = (uv)^p = u^p v^p = \varphi(u)\varphi(v)$ shows that φ respects products. If u and v are in $\mathbb{k}$, then

$$\varphi(u+v) = (u+v)^p = \varphi(u) + \sum_{j=1}^{p-1} \tbinom{p}{j} u^{p-j} v^j + \varphi(v) = \varphi(u) + \varphi(v),$$

the last equality holding since the binomial coefficient $\binom{p}{j}$ has a p in the numerator for $1 \leq j \leq p-1$. Thus φ is a ring homomorphism. Since $\varphi(1) = 1$, φ is a field mapping.

PROOF OF UNIQUENESS IN THEOREM 9.14. Let $\Bbbk$ be a finite field, say of characteristic p, and let $\mathbb{P}$ be the prime field of order p within $\Bbbk$. We know that $\mathbb{P}$ is isomorphic to $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Since $\Bbbk$ is a finite-dimensional vector space over $\mathbb{P}$, we know also that $\Bbbk$ has order $q = p^n$ for some integer $n > 0$. The multiplicative group $\Bbbk^\times$ of $\Bbbk$ thus has order $q - 1$, and every $x \neq 0$ in $\Bbbk$ therefore satisfies $x^{q-1} = 1$. Taking $x = 0$ into account, we see that every member of $\Bbbk$ satisfies $x^q = x$. Forming the polynomial $X^q - X$ in $\mathbb{P}[X]$, we see that every member of $\Bbbk$ is a root of this polynomial. Iterated application q times of the Factor Theorem (Corollary 1.13) shows that $X^q - X$ factors into degree-one factors in $\Bbbk$. Since every member of $\Bbbk$ is a root of $X^q - X$, $\Bbbk$ is a splitting field of $X^q - X$ over $\mathbb{P}$. Then the uniqueness of the prime field up to isomorphism, in combination with the uniqueness of the splitting field of $X^q - X$ given in Theorem 9.13′, shows that $\Bbbk$ is uniquely determined up to isomorphism. □

PROOF OF EXISTENCE IN THEOREM 9.14. Let $q = p^n$ be given, and define $\Bbbk$ to be a splitting field of $X^q - X$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The field $\Bbbk$ exists by Theorem 9.12, and it has characteristic p. Since $X^q - X$ is monic of degree q, the definition of splitting field says that we can write

$$X^q - X = (X - u_1)(X - u_2)\cdots(X - u_q) \qquad \text{with all } u_j \in \Bbbk.$$

Because of Lemma 9.18, the map $\varphi(u) = u^q$, which is the n^{th} power of the map $u \mapsto u^p$, is a field mapping of $\Bbbk$ into itself. The members of $\Bbbk$ fixed by φ form a subfield of $\Bbbk$, and these elements of $\Bbbk$ are exactly the members of the set $S = \{u_1, \ldots, u_q\}$. Therefore S is a subfield of $\Bbbk$, necessarily containing $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Since $X^q - X$ splits in S and since the roots of $X^q - X$ generate S, S is a splitting field of $X^q - X$ over $\mathbb{F}_p$. In other words, $S = \Bbbk$. To complete the proof, it is enough to show that the elements $u_1, \ldots, u_q$ are distinct, and then $\Bbbk$ will be a field of q elements. The question is therefore whether some root of $X^q - X$ has multiplicity at least 2, i.e., whether $(X - r)^2$ divides $X^q - X$ for some r in $\Bbbk$. Corollary 9.17 gives a necessary condition for this divisibility, saying that the derivative of $X^q - X$ must have r as a root. However, the derivative of $X^q - X$ is $qX^{q-1} - 1 = -1$, and the constant polynomial -1 has no roots. We conclude that $\Bbbk$ has q elements. □

Corollary 9.19. If q and r are integers with $2 \leq q \leq r$, then the finite field $\mathbb{F}_q$ is isomorphic to a subfield of the finite field $\mathbb{F}_r$ if and only if $r = q^n$ for some integer $n \geq 1$.

PROOF. If $\mathbb{F}_q$ is isomorphic to a subfield of $\mathbb{F}_r$, then we may consider $\mathbb{F}_r$ as a vector space over $\mathbb{F}_q$, say of dimension n. In this case, $\mathbb{F}_r$ has q^n elements.

Conversely let $r = q^n$, and regard $\mathbb{F}_r$ as a splitting field of $X^{q^n} - X$ over the prime field $\mathbb{F}_p$, by Theorem 9.14. Let S be the subset of $\mathbb{F}_r$ of all roots of $X^q - X$.

Pure Mathematical Physics

Putting $a = q - 1$ and $k = \frac{q^n-1}{q-1} = q^{n-1} + q^{n-2} + \cdots + 1$, we have

$$X^{ka} - 1 = (X^a - 1)(X^{(k-1)a} + X^{(k-2)a} + \cdots + 1).$$

Multiplying by X, we see that $X^q - X$ is a factor of $X^{q^n} - X$. Since $X^{q^n} - X$ splits in $\mathbb{F}_r$ and has distinct roots, the same is true of $X^q - X$. Therefore $|S| = q$.

Let $q = p^m$. The m^{th} power of the homomorphism of Lemma 9.18 on $\Bbbk = \mathbb{F}_r$ is $x \mapsto x^q$, and the subset of $\mathbb{F}_r$ fixed by this homomorphism is a subfield. Thus S is a subfield, and it has q elements. □

4. Algebraic Closure

Algebraically closed fields—those for which every nonconstant polynomial with coefficients in the field has a root in the field—were introduced in Section V.1, and it was mentioned at that time that every field is a subfield of some algebraically closed field. We shall prove that existence theorem in this section in a form lending itself to a uniqueness result.

Throughout this section let $\Bbbk$ be a field. We begin by giving further descriptions of algebraically closed fields that take the theory of Sections 1–2 into account.

Proposition 9.20. The following conditions on the field $\Bbbk$ are equivalent:

(a) $\Bbbk$ has no nontrivial algebraic extensions,
(b) every irreducible polynomial in $\Bbbk[X]$ has degree 1,
(c) every polynomial in $\Bbbk[X]$ of positive degree has at least one root in $\Bbbk$,
(d) every polynomial in $\Bbbk[X]$ of positive degree factors over $\Bbbk$ into polynomials of degree 1.

PROOF. If (a) holds, then (b) holds since any irreducible polynomial of degree greater than 1 would give a nontrivial simple algebraic extension (Theorem 9.10). If (b) holds and a polynomial of positive degree is given, apply (b) to an irreducible factor to see that the given polynomial has a root; thus (c) holds. Condition (c) implies condition (d) by induction and the Factor Theorem. If (d) holds and if $\mathbb{K}$ is an algebraic extension of $\Bbbk$, let x be in $\mathbb{K}$, and let $F(X)$ be the minimal polynomial of x over $\Bbbk$. Then $F(X)$ is irreducible over $\Bbbk$, and (d) says that $F(X)$ has degree 1. Hence x is in $\Bbbk$, and we conclude that $\mathbb{K} = \Bbbk$. □

A field satisfying the equivalent conditions of Proposition 9.20 is said to be **algebraically closed**.

EXAMPLES OF ALGEBRAICALLY CLOSED FIELDS.

(1) The Fundamental Theorem of Algebra (Theorem 1.18) says that $\mathbb{C}$ is algebraically closed. This theorem was not proved in Chapter I, but a proof will be given in this chapter in Section 10.

(2) Let $\mathbb{K}$ be the subset of all members of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$. By Corollary 9.9, $\mathbb{K}$ is a subfield of $\mathbb{C}$. Example 1 shows that every polynomial in $\mathbb{Q}[X]$ splits in $\mathbb{K}$, and Lemma 9.21 below then allows us to conclude that $\mathbb{K}$ is algebraically closed.

(3) Fix a prime number p, and start with $\Bbbk_0 = \mathbb{F}_p$ as the prime field $\mathbb{Z}/p\mathbb{Z}$. Enumerate the members of $\mathbb{F}_p[X]$, letting $F_n(X)$ be the n^{th} such polynomial. We construct $\Bbbk_n$ by induction on n so that $\Bbbk_n$ is a splitting field for $F_n(X)$ over $\Bbbk_{n-1}$ when $n \geq 1$. Then $\Bbbk_0 \subseteq \Bbbk_1 \subseteq \Bbbk_2 \subseteq \cdots$ is an increasing sequence of fields containing $\mathbb{F}_p$. Let $\mathbb{K}$ be the union. Any two elements of $\mathbb{K}$ lie in a single $\Bbbk_n$, and it follows that $\mathbb{K}$ is closed under the field operations. Any three elements lie in a single $\Bbbk_n$, and it follows that any of the defining properties of a field is valid in $\mathbb{K}$ because it is valid in $\Bbbk_n$. Therefore $\mathbb{K}$ is a field. This field is an extension of $\mathbb{F}_p$, and every polynomial in $\mathbb{F}_p[X]$ splits in $\mathbb{K}$. As in Example 2, Lemma 9.21 below shows that $\mathbb{K}$ is algebraically closed.

Lemma 9.21. If $\mathbb{K}/\Bbbk$ is an algebraic extension of fields and if every nonconstant polynomial in $\Bbbk[X]$ splits into degree-one factors in $\mathbb{K}$, then $\mathbb{K}$ is algebraically closed.

PROOF. Let $\mathbb{K}'$ be an algebraic extension of $\mathbb{K}$, and let x be in $\mathbb{K}'$. Let $G(X)$ be the minimal polynomial of x over $\mathbb{K}$, and write $G(X)$ as

$$G(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0 \qquad \text{with all } c_i \in \mathbb{K}.$$

Then x is algebraic over $\Bbbk(c_{n-1}, \ldots, c_0)$, which is a finite extension of $\Bbbk$ by Theorem 9.8. By Corollary 9.7, x lies in a finite extension of $\Bbbk$. Thus Proposition 9.4 shows that x is algebraic over $\Bbbk$. Let $F(X)$ be the minimal polynomial of x over $\Bbbk$. By assumption this splits over $\mathbb{K}$, say as

$$F(X) = (X - x_1)\cdots(X - x_m) \qquad \text{with all } x_i \in \mathbb{K}.$$

Evaluating at x and using the fact that $F(x) = 0$, we see that $x = x_j$ for some j. Therefore x is in $\mathbb{K}$, and $\mathbb{K}$ is algebraically closed. □

An extension field $\mathbb{K}/\Bbbk$ is an **algebraic closure** of $\Bbbk$ if $\mathbb{K}$ is algebraic over $\Bbbk$ and if $\mathbb{K}$ is algebraically closed. Example 2 of algebraically closed fields above gives an algebraic closure of $\mathbb{Q}$, and Example 3 gives an algebraic closure of $\mathbb{F}_p$.

Pure Mathematical Physics

Theorem 9.22 (Steinitz). Every field $\Bbbk$ has an algebraic closure, and this is unique up to $\Bbbk$ isomorphism.

REMARKS. The proof of existence is modeled on the argument for Example 3 of algebraic closures. However, we are not free in general to use a simple union of a sequence of fields and have to work harder. Because there is no evident set of possibilities within which we are forming extension fields, Zorn's Lemma is inconvenient to use and tends to result in an unintuitive construction. Instead, we use Zermelo's Well-Ordering Theorem, whose use more closely parallels the inductive construction in Example 3.

PROOF OF EXISTENCE. With $\Bbbk$ as the given field, let S be the set of nonconstant polynomials $s(X)$ in $\Bbbk[X]$, and introduce a well ordering into S by means of Zermelo's Well-Ordering Theorem (Section A5 of the appendix). Let us write $\prec$ for "strictly precedes in the ordering" and $\precsim$ for "equals or strictly precedes." For each $s \in S$, let $\bar{s}$ be the successor of s, i.e., the first element among all elements t with $s \prec t$. We write s_0 for the first element of S. Without loss of generality, we may assume that S has a last element s_∞. The idea is to construct simultaneously two kinds of things:

(i) an algebraic extension field $\Bbbk_s/\Bbbk$ for each $s \in S$ such that $\Bbbk_{s_0} = \Bbbk$ and such that $\Bbbk_{\bar{s}}$ is a splitting field for $s(X)$ over $\Bbbk_s$ whenever $s \prec s_\infty$,

(ii) a field mapping $\varphi_{ut} : \Bbbk_t \to \Bbbk_u$ for each ordered pair of elements t and u in S having $t \precsim u$, such that $\varphi_{tt} = 1$ for all t and such that $t \precsim u \precsim v$ implies $\varphi_{vt} = \varphi_{vu}\varphi_{ut}$.

These extension fields and mappings are to be such that $\Bbbk_s = \bigcup_{t \prec s} \varphi_{st}(\Bbbk_t)$ whenever s is not a successor and is not s_0. If such a system of extension fields and field homomorphisms exists, then Lemma 9.21 applies to a splitting field over $\Bbbk_{s_\infty}$ of the nonconstant polynomial $s_\infty(X)$ and shows that this splitting field is algebraically closed; since this splitting field is an algebraic extension of $\Bbbk$, it is an algebraic closure of $\Bbbk$.

A partial such system through t_0 means a system consisting of fields $\Bbbk_s$ with $s \precsim t_0$ and field homomorphisms φ_{ut} with $t \precsim u \precsim t_0$ such that the above conditions hold as far as they are applicable. A partial system exists through the first member s_0 of S because we can take $\Bbbk_{s_0} = \Bbbk$ and $\varphi_{s_0 s_0} = 1$. Arguing by contradiction, we suppose that such a system of extension fields and field homomorphisms fails to exist through some member of S. Let t_0 be the first member of S such that there is no partial system through t_0.

Suppose that t_0 is the successor of some element t_1 in S. We know that a partial system exists through t_1. If we let $\Bbbk_{t_0}$ be a splitting field for $t_1(X)$ over $\Bbbk_{t_1}$, and if we define

$$\varphi_{t_0 t} = \begin{cases} \varphi_{t_0 t_1}\varphi_{t_1 t} & \text{for } t \precsim t_1, \\ 1 & \text{for } t = t_0, \end{cases}$$

Pure Mathematical Physics

then the enlarged system is a partial system through t_0, contradiction. Thus t_0 cannot be the successor of some element of S.

When t_0 is not a successor, at least $\mathbb{k}_t$ is defined for $t \prec t_0$ and φ_{ut} is defined for $t \precsim u \prec t_0$. We want to form a union, but we have to keep the field operations aligned properly in the process. Define a "t-allowable tuple" to be a function $u \mapsto x_u$ defined for $t \precsim u \prec t_0$ such that x_u is in $\mathbb{k}_u$ and $\varphi_{vu}(x_u) = x_v$ whenever $t \precsim u \precsim v \prec t_0$. If x is in $\mathbb{k}_t$, then an example of a t-allowable tuple is given by $u \mapsto \varphi_{ut}(x)$ for $t \precsim u \prec t_0$.

If $t \prec t_0$ and $t' \prec t_0$, then we can apply field operations to the t-allowable tuple $u \mapsto x_u$ and to the t'-allowable tuple $u \mapsto y_u$, obtaining $\max(t, t')$-allowable tuples $u \mapsto x_u + y_u$, $u \mapsto -x_u$, $u \mapsto x_u y_u$, and $x_u \mapsto x_u^{-1}$ as long as $x_t \neq 0$. These operations are meaningful since each φ_{vu} is a field mapping.

If $t \prec t_0$ and $t' \prec t_0$, we say that the t-allowable tuple $u \mapsto x_u$ is equivalent to the t'-allowable tuple $u \mapsto y_u$ if $x_u = y_u$ for $\max(t, t') \precsim u \prec t_0$. The result is an equivalence relation, and the equivalence relation respects the field operations in the previous paragraph. We define $\mathbb{k}_{t_0}$ to be the set of equivalence classes of allowable tuples with the inherited field operations. The 0 element is the class of the s_0-allowable tuple $u \mapsto 0$, and the multiplicative identity is the class of the s_0-allowable tuple $u \mapsto 1$. It is a routine matter to check that $\mathbb{k}_{t_0}$ is a field.

If $t \prec t_0$ is given, we define the function $\varphi_{t_0 t} : \mathbb{k}_t \to \mathbb{k}_{t_0}$ as follows: if x is in $\mathbb{k}_t$, we form the t-allowable tuple $u \mapsto \varphi_{ut}(x)$ and take its equivalence class, which is a member of $\mathbb{k}_{t_0}$, as $\varphi_{t_0 t}(x)$. Then $\varphi_{t_0 t}$ is evidently a field mapping. It is evident also that $\varphi_{t_0 v}\varphi_{vu} = \varphi_{t_0 u}$ when $u \precsim v \prec t_0$. Defining $\varphi_{t_0 t_0}$ to be the identity, we have a complete system of field mappings φ_{vu} for $\mathbb{k}_{t_0}$.

The final step is to check that $\mathbb{k}_{t_0}$ is the union of the images of the $\varphi_{t_0 t}$ for $t \prec t_0$. Thus choose a representative of an equivalence class in $\mathbb{k}_{t_0}$. Let the representative be a t-allowable tuple $u \mapsto x_u$ for $t \precsim u \prec t_0$. The element x_t is in $\mathbb{k}_t$, and the condition $x_u = \varphi_{ut}(x_t)$ is just the condition that the class of $u \mapsto x_u$ be the image of x_t under $\varphi_{t_0 t}$. Hence every member of $\mathbb{k}_{t_0}$ is in the image of some $\varphi_{t_0 t}$ with $t \prec t_0$, and we have a contradiction to the hypothesis that a partial system through t_0 does not exist. This completes the proof of existence. □

For the uniqueness in Theorem 9.22, we again need a serious application of the Axiom of Choice, but here Zorn's Lemma can be applied fairly routinely. The proof will show a little more than is needed, and in fact the uniqueness in Theorem 9.22 will be derived as a consequence of Theorem 9.23 below.

Theorem 9.23. Let $\mathbb{K}'$ be an algebraically closed field, and let $\mathbb{K}$ be an algebraic extension of a field $\mathbb{k}$. If φ is a field mapping of $\mathbb{k}$ into $\mathbb{K}'$, then φ can be extended to a field mapping of $\mathbb{K}$ into $\mathbb{K}'$.

PROOF OF UNIQUENESS IN THEOREM 9.22 USING THEOREM 9.23. Let $\mathbb{K}$ and $\mathbb{K}'$ be algebraic closures of $\Bbbk$, and let $\varphi : \Bbbk \to \mathbb{K}'$ be the inclusion mapping. Theorem 9.23 supplies a field mapping $\Phi : \mathbb{K} \to \mathbb{K}'$ such that $\Phi\big|_{\Bbbk} = \varphi$, i.e., such that Φ fixes $\Bbbk$. Since $\mathbb{K}$ is an algebraic closure of $\Bbbk$, so is $\Phi(\mathbb{K})$. Then $\mathbb{K}'$ is an algebraic extension of the algebraically closed field $\Phi(\mathbb{K})$, and we must have $\Phi(\mathbb{K}) = \mathbb{K}'$. Thus Φ is a $\Bbbk$ isomorphism of $\mathbb{K}$ onto $\mathbb{K}'$.

PROOF OF THEOREM 9.23. Let S be the set of all triples $(\mathbb{L}, \mathbb{L}', \psi)$ such that $\mathbb{L}$ is a field with $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$ and ψ is a field mapping of $\mathbb{L}$ onto the subfield $\mathbb{L}'$ of $\mathbb{K}'$ with $\psi\big|_{\Bbbk} = \varphi$. The set S is nonempty since $(\Bbbk, \varphi(\Bbbk), \varphi)$ is a member of it. Defining $(\mathbb{L}_1, \mathbb{L}'_1, \psi_1) \subseteq (\mathbb{L}_2, \mathbb{L}'_2, \psi_2)$ to mean that $\mathbb{L}_1 \subseteq \mathbb{L}_2$, that $\mathbb{L}'_1 \subseteq \mathbb{L}'_2$, and that ψ_1 as a set of ordered pairs is a subset of ψ_2 as a set of ordered pairs, we partially order S by inclusion upward. If $\{(\mathbb{L}_\alpha, \mathbb{L}'_\alpha, \psi_\alpha)\}$ is a nonempty chain in S, form the triple $\big(\bigcup_\alpha \mathbb{L}_\alpha, \bigcup_\alpha \mathbb{L}'_\alpha, \bigcup_\alpha \psi_\alpha\big)$, and put $\psi = \bigcup_\alpha \psi_\alpha$. Then $\psi\big(\bigcup_\alpha \mathbb{L}_\alpha\big) = \bigcup_\alpha \mathbb{L}'_\alpha$, and consequently $\big(\bigcup_\alpha \mathbb{L}_\alpha, \bigcup_\alpha \mathbb{L}'_\alpha, \bigcup_\alpha \psi_\alpha\big)$ is an upper bound in S for the chain. By Zorn's Lemma, S has a maximal element $(\mathbb{L}_0, \mathbb{L}'_0, \psi_0)$. We shall prove that $\mathbb{L}_0 = \mathbb{K}$, and the proof will be complete.

Fix x in $\mathbb{K}$, and let $F(X)$ be the minimal polynomial of x over $\mathbb{L}_0$. The minimal polynomial of $\psi_0(x)$ over $\mathbb{L}'_0$ is then $F^{\psi_0}(X)$. Since $\mathbb{K}'$ is algebraically closed, $F^{\psi_0}(X)$ has a root x' in $\mathbb{K}'$. By Theorem 9.11′, $\psi_0 : \mathbb{L}_0 \to \mathbb{L}'$ can be extended to an isomorphism $\Psi_0 : \mathbb{L}_0(x) \to \mathbb{L}'_0(x')$ such that $\psi_0(x) = x'$. Then $(\mathbb{L}_0(x), \mathbb{L}'_0(x'), \Psi_0)$ is in S and contains $(\mathbb{L}_0, \mathbb{L}'_0, \psi_0)$. This containment, if strict, would contradict the fact that $(\mathbb{L}_0, \mathbb{L}'_0, \psi_0)$ is a maximal element of S. Thus equality must hold: $\mathbb{L}_0(x) = \mathbb{L}_0$. Therefore x is in $\mathbb{L}_0$, and we conclude that $\mathbb{L}_0 = \mathbb{K}$. □

The use of algebraic closures allows us to simplify understanding of splitting fields. If we are working with a field $\Bbbk$ and is $\overline{\Bbbk}$ is a fixed algebraic closure of $\Bbbk$, then the existence and uniqueness of *the* splitting field of a polynomial $F(X)$ in $\Bbbk[X]$ becomes evident; no isomorphisms are involved. Namely let $\alpha_1, \ldots, \alpha_n$ be the roots of $F(X)$ in $\overline{\Bbbk}$. Then the subfield of $\overline{\Bbbk}$ generated by $\Bbbk$ and $\alpha_1, \ldots, \alpha_n$ is the splitting field of $F(X)$, and it is manifestly unique. Henceforth when we refer to *the* splitting field of a polynomial over a field $\Bbbk$, it is with an understanding of working within a fixed algebraic closure in this way.

5. Geometric Constructions by Straightedge and Compass

Classical Euclidean geometry attached a certain emphasis to constructions in the Euclidean plane that could be made by straightedge and compass. These are often referred to casually as constructions by "ruler and compass," but one is not

Pure Mathematical Physics

allowed to use the markings on a ruler. Thus "straightedge and compass" is a more accurate description.

In these constructions the starting configuration may be regarded as a line with two points marked on the line. Allowable constructions are the following: to form the line through a given point different from finitely many other lines through that point, to form the line through two distinct points, to form a circle with a given center and a radius different from that of finitely many other circles through the point, and to form a circle with a given center and radius. Intersections of a line or a circle with previous lines and circles establish new points for continuing the construction.

For example a line perpendicular to a given line at a given point can be constructed by drawing any circle centered at the point, using the two intersection points as centers of new circles, drawing those circles so as to have radius larger than the first circle, and forming the line between their two points of intersection. An angle at the point P of intersection between two intersecting lines A and B may be bisected by drawing any circle centered at P, selecting one of the points of intersection on each line so that P and the two new points Q and R describe the angle, drawing circles with that same radius centered at Q and R, and forming the line between the points of intersection of the two circles. And so on.

Three notable problems remained unsolved in antiquity:

(i) how to double a cube, i.e., how to construct the side of a cube of double the volume of a given cube,

(ii) how to trisect any constructible angle, i.e., how to divide the angle into three equal parts by means of constructed lines,

(iii) how to square a circle, i.e., how to construct the side of a square whose area equals that of a given disk.

In this section we shall use the elementary field theory of Sections 1–2 to show that doubling a cube and trisecting a 60-degree angle are impossible with straightedge and compass. As to (iii), we shall reduce a proof of the impossibility of squaring the circle to a proof that π is transcendental over $\mathbb{Q}$. This latter proof we give in Section 14.

The first step is to translate the problem of geometric constructibility into a statement in algebra. Since we are given two points on a line, we can introduce Cartesian coordinates for the Euclidean plane, taking one of the points to be $(0, 0)$ and the other point to be $(1, 0)$. Points in the Euclidean plane are now determined by their Cartesian coordinates, which determine all distances. Distances in turn can be laid off on the x-axis from $(0, 0)$. Thus the question becomes, what points on the x-axis can be constructed?

Let $\mathcal{C}$ be the set of constructible x coordinates. We are given that 0 and 1 are in $\mathcal{C}$. Closure of $\mathcal{C}$ under addition and subtraction is evident; the straightedge is not even necessary for this step. Figure 9.1 indicates why the positive elements

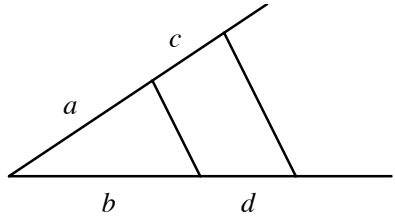


FIGURE 9.1. Closure of positive constructible x coordinates under multiplication and division.

of $\mathcal{C}$ are closed under multiplication and division. In more detail we take two intersecting lines and mark three known positive members of $\mathcal{C}$ as the distances a, b, c in the figure. Then we form the line through the two points marking a and b, and we form a line parallel to that line through the point marked off by the distance c. The intersection of this parallel line with the other original line defines a distance d. Then $a/b = c/d$, and so $d = bc/a$. By taking $a = 1$, we see that we can multiply any two members b and c in $\mathcal{C}$, obtaining a result in $\mathcal{C}$. By instead taking $c = 1$, we see that we can divide. The conclusion is that $\mathcal{C}$ is a field.

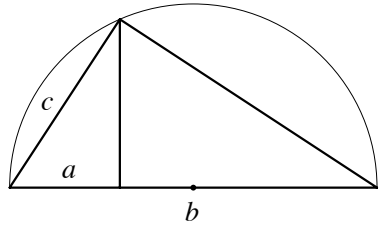


FIGURE 9.2. Closure of positive constructible x coordinates under square roots.

Figure 9.2 indicates why the positive elements of $\mathcal{C}$ are closed under taking square roots. In more detail let a and b be positive members of $\mathcal{C}$ with $a < b$. By forming a circle whose diameter is a segment of length b and by forming a line perpendicular to that line at the point marked by a, we determine the pictured right triangle with a side c satisfying $a/c = c/b$. Then $c = \sqrt{ab}$. By taking one of a and b to be 1, we see that the square root of the other of a and b is in $\mathcal{C}$. This completes the proof of the direct part of the following theorem.

Theorem 9.24. The set $\mathcal{C}$ of x coordinates that can be constructed from $x = 1$ and $x = 0$ by straightedge and compass forms a subfield of $\mathbb{R}$ such that the square

root of any positive element of the field lies in the field. Conversely the members of $\mathcal{C}$ are those real numbers lying in some subfield F_n of $\mathbb{R}$ of the form

$$F_1 = \mathbb{Q}(\sqrt{a_0}), \quad F_2 = F_1(\sqrt{a_1}), \quad \dots, \quad F_n = F_{n-1}(\sqrt{a_{n-1}})$$

with each a_j in F_j and with $a_0, \dots, a_{n-1}$ all ≥ 0.

PROOF OF CONVERSE. Suppose we have a subfield $F = F_n$ of $\mathbb{R}$ of the kind described in the statement of the theorem. The possibilities for obtaining a new constructible point from F by an additional construction arise from three situations: the intersection of two lines, each passing through two points of F; the intersection of a line and a circle, each determined by data from F; and the intersection of two circles, each determined by data from F.

In the case of two intersecting lines, each line is of the form $ax + by = c$ for suitable coefficients a, b, c in F, and the intersection is a point (x, y) in $F \times F$. So intersections of lines do not force us to enlarge F.

For a line and a circle, we assume that the line is given by $ax + by = c$ with a, b, c in F, that the circle has radius in F and center in $F \times F$, and that the lines and the circle actually intersect. The circle is then given by $(x-h)^2+(y-k)^2 = r^2$ with h, k, r in F. Substitution of the equation of the line into the equation of the circle gives us a quadratic equation either for x, and x then determines y, or for y, and y then determines x. The quadratic equation has real roots, and thus its discriminant is ≥ 0. The result is that x and y are in a field $F(\sqrt{l}\,)$ for some $l \geq 0$ in F.

For two circles, without loss of generality, we may take their equations to be

$$x^2 + y^2 = r^2 \qquad \text{and} \qquad (x-h)^2 + (y-h)^2 = s^2$$

with r, h, k, s in F. Subtracting gives $2xh + 2yk = h^2 + k^2 - s^2 + r^2$. With this equation and with $x^2 + y^2 = r^2$, we again have a line and circle that are being intersected. Thus the same remarks apply as in the previous paragraph.

The conclusion is that any new single construction of points of intersection by straightedge and compass leads from F to $F(\sqrt{l}\,)$ for some $l \geq 0$ in F. Thus every member of the set $\mathcal{C}$ is as described in the theorem. □

To apply the theorem to prove the impossibility of the three never-accomplished constructions that were described earlier in the section, we observe that $[F_i : F_{i-1}]$ in the theorem equals 1 or 2 for each i. Consequently every member of the constructible set $\mathcal{C}$ lies in a finite algebraic extension of $\mathbb{Q}$ of degree 2^k for some k.

For the problem of doubling a cube, the question amounts to constructing $\sqrt[3]{2}$. We argue by contradiction. If $\sqrt[3]{2}$ lies in F_n as in the theorem, then $\mathbb{Q}(\sqrt[3]{2}\,) \subseteq F_n$. With k as the integer $\leq n$ such that $[F_n : \mathbb{Q}] = 2^k$, Corollary 9.7 gives

$$2^k = [F_n : \mathbb{Q}] = [F_n : \mathbb{Q}(\sqrt[3]{2}\,)]\,[\mathbb{Q}(\sqrt[3]{2}\,) : \mathbb{Q}] = 3[F_n : \mathbb{Q}(\sqrt[3]{2}\,)].$$

Thus 3 must divide a power of 2, and we have arrived at a contradiction. We conclude that it is not possible to double a cube with straightedge and compass.

For the problem of trisecting any constructible angle, let us show that a 60° angle cannot be trisected. A 60° angle is itself constructible, being the angle between two sides in an equilateral triangle. Trisecting a 60° angle amounts to constructing $\cos 20^\circ$; $\sin 20^\circ$ is then $(1 - \cos^2 20^\circ)^{1/2}$. To proceed, we derive an equation satisfied by $\cos 20^\circ$, starting from

$$(\cos 20^\circ + i \sin 20^\circ)^3 = \cos 60^\circ + i \sin 60^\circ = \tfrac{1}{2} + \tfrac{i\sqrt{3}}{2}.$$

We expand the left side and extract the real part of both sides to obtain

$$\cos^3 20^\circ - 3 \cos 20^\circ \sin^2 20^\circ = \tfrac{1}{2}.$$

Substituting $\sin^2 20^\circ = 1 - \cos^2 20^\circ$ and simplifying, we see that $r = \cos 20^\circ$ satisfies

$$4r^3 - 3r - \tfrac{1}{2} = 0.$$

Arguing with Corollary 8.20 as in Example 2 of splitting fields in Section 2, we readily check that $4X^3 - 3X - \frac{1}{2}$ is irreducible over $\mathbb{Q}$. Hence $[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = 3$, and we are led to the same contradiction as for the problem of doubling the cube. Therefore it is not possible to trisect a 60° angle with straightedge and compass.

For the problem of squaring a circle, let A be the area of the circle, and let r be the radius. If the square has side x, then $x^2 = A = \pi r^2$, with r given. Thus $x = r\sqrt{\pi}$, and the essence of the matter is to construct $\sqrt{\pi}$. However, π is known to be transcendental by a theorem of F. Lindemann (1882); we give a proof in Section 14. Since π is transcendental, $\sqrt{\pi}$ is transcendental.

A fourth notable problem, which leads to further insights, concerns the construction of a regular polygon of outer radius 1 with n sides. This construction is easy with straightedge and compass when n is a power of 2 or is 3 times a power of 2, and Euclid showed that a construction is possible for $n = 5$. But a construction cannot be managed with straightedge and compass for $n = 9$, for example, because a central angle in this case is 40° and the constructibility of $\cos 40^\circ$ would imply the constructibility of $\cos 20^\circ$. Thus the question is, for what values of n can a regular n-gon be constructed with straightedge and compass?

The remarkable answer was given by Gauss. By a **Fermat number** is meant any integer of the form $2^{2^N} + 1$. A **Fermat prime** is a Fermat number that is prime. The Fermat numbers for $N = 0, 1, 2, 3, 4$ are $3, 5, 17, 257, 65537$, and each is a Fermat prime. No larger Fermat primes are known.[2] The answer given

[2]Many Fermat numbers for $N \geq 5$ are known not to be prime, sometimes by the discovery of an explicit factor and sometimes by a verification that 3 to the power 2^{2^N-1} is not congruent to -1 modulo $(2^{2^N} + 1)$. (Cf. Lemma 9.46.) For example Euler discovered that 641 divides $2^{2^5} + 1$. Computer calculations have shown that 2^{2^N+1} is not prime if $5 \leq N \leq 32$.

by Gauss, which we shall prove in stages in Sections 6–9, is as follows.

Theorem 9.25 (Gauss).[3] A regular n-gon is constructible with straightedge and compass if and only if n is the product of distinct Fermat primes and a power of 2.

We can show the relevance of Fermat primes right now, and we can give an indication that if n is a prime number, then a regular n-gon can be constructed if and only if n is a Fermat prime. But a full proof even of this statement will make use of Galois groups, which we take up in the next three sections.

For the necessity let n be prime, and suppose that a regular n-gon is constructible. Returning from degrees to radians, we observe that each central angle is $2\pi/n$. Thus the constructibility implies the constructibility of $\cos 2\pi/n$, and it follows that $e^{2\pi i/n} = \cos 2\pi/n + i \sin 2\pi/n$ is in the field $\mathcal{C} + i\mathcal{C}$ of constructible points in the complex plane. We have the factorization

$$X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + \cdots + X + 1).$$

and $e^{2\pi i/n}$ is a root of the second factor. The first example of Eisenstein's criterion (Corollary 8.22) in Section VIII.5 shows that the second factor is irreducible. According to the results of Section 1, $\mathbb{Q}(e^{2\pi i/n})$ is a simple algebraic extension of $\mathbb{Q}$ of degree $n - 1$.

Applying Theorem 9.24, we see that $n - 1$ must be a power of two. Let us write $n - 1 = 2^m$. Suppose $m = a2^N$ with a odd. If $a > 1$, then the equality $n = 2^{a2^N} + 1 = (2^{2^N})^a + 1^a$ exhibits n as the sum of two a^{th} powers, necessarily divisible by $2^{2^N} + 1$. Since n is assumed prime, we conclude that $a = 1$. Therefore $n = 2^{2^N} + 1$, and n is a Fermat prime.

We do not quite succeed in proving the converse at this point. If n is the Fermat prime $2^{2^N} + 1$, then the above argument shows that the degree of $\mathbb{Q}(e^{2\pi i/n})$ over $\mathbb{Q}$ is 2^{2^N}. However, we cannot yet conclude that $\mathbb{Q}(e^{2\pi i/n})$ can be built from $\mathbb{Q}$ by successively adjoining 2^N square roots, and thus the converse part of Theorem 9.24 is not immediately applicable. Once we have the theory of Galois groups in hand, we shall see that the existence of these intermediate extensions involving square roots is ensured, and then the constructibility follows.

[3]Gauss announced both the necessity and the sufficiency in this theorem in his *Disquisitiones Arithmeticae* in 1801, but he included a proof of only the sufficiency (partly in his articles 336 and 365). A proof of the necessity appeared in a paper of Pierre-Laurent Wantzel in 1837.

Pure Mathematical Physics

6. Separable Extensions

The **Galois group** $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ of a field extension $\mathbb{K}/\Bbbk$ is defined to be the set

$$\mathrm{Gal}(\mathbb{K}/\Bbbk) = \{\Bbbk \text{ automorphisms of } \mathbb{K}\}$$

with composition as group operation. An instance of this group was introduced in the context of Example 9 of Section IV.1; in this example the field $\Bbbk$ was the field $\mathbb{Q}$ of rationals and the field $\mathbb{K}$ was a number field $\mathbb{Q}[\theta]$, where θ is algebraic over $\mathbb{Q}$. In studying $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ in this chapter, we ordinarily assume that $\dim_{\Bbbk} \mathbb{K} < \infty$, but there will be instances where we do not want to make such an assumption.

Beginning in this section, we take up a study of Galois groups in general. We shall be interested in relationships between fields $\mathbb{L}$ with $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$ and subgroups of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. If H is a subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, then

$$\mathbb{K}^H = \left\{x \in \mathbb{K} \mid \varphi(x) = x \text{ for all } \varphi \in H\right\}$$

is a field called the **fixed field** of H; it provides an example of an intermediate field $\mathbb{L}$ and gives a hint of the relationships we shall investigate. We begin with some examples; in each case the base field $\Bbbk$ is the field $\mathbb{Q}$ of rationals.

EXAMPLES OF GALOIS GROUPS.

(1a) $\mathbb{K} = \mathbb{Q}(\sqrt{-1}\,)$. If φ is in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, then we must have $\varphi\big|_{\mathbb{Q}} = 1$, and $\varphi(\sqrt{-1}\,)$ must be a root of $X^2 + 1$. Thus $\varphi(\sqrt{-1}\,) = \pm\sqrt{-1}$. Since $\mathbb{Q}$ and $\sqrt{-1}$ generate $\mathbb{Q}(\sqrt{-1}\,)$, there are at most two such φ's. On the other hand, $\mathbb{Q}(\sqrt{-1}\,)$ and $\mathbb{Q}(-\sqrt{-1}\,)$ are simple extensions of $\mathbb{Q}$ such that $\sqrt{-1}$ and $-\sqrt{-1}$ have the same minimal polynomial. Theorem 9.11 therefore produces a $\mathbb{Q}$ automorphism of $\mathbb{Q}(\sqrt{-1}\,)$ with $\varphi(\sqrt{-1}\,) = -\sqrt{-1}$, namely complex conjugation. We conclude that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ has order 2, hence that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong C_2$.

(1b) $\mathbb{K} = \mathbb{Q}(\sqrt{2}\,)$. The same argument applies as in Example 1a, and the conclusion is that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong C_2$. The nontrivial element of the Galois group carries $\sqrt{2}$ to $-\sqrt{2}$ and is different from complex conjugation.

(2) $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}\,)$. If φ is in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, then $\varphi\big|_{\mathbb{Q}} = 1$, and $\varphi(\sqrt[3]{2}\,)$ has to be a root of $X^3 - 2$. But $\mathbb{K}$ is a subfield of $\mathbb{R}$, and there is only one root of $X^3 - 2$ in $\mathbb{R}$. Hence $\varphi(\sqrt[3]{2}\,) = \sqrt[3]{2}$. Since $\mathbb{Q}$ and $\sqrt[3]{2}$ generate $\mathbb{Q}(\sqrt[3]{2}\,)$ as a field, we see that $\varphi = 1$. We conclude that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ has order 1, i.e., is the trivial group.

(3) $\mathbb{K} = \mathbb{Q}(r)$, where r is a root of $X^3 - X - \frac{1}{3}$. Any φ in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ fixes $\mathbb{Q}$ and sends r to a root of $X^3 - X - \frac{1}{3}$. In Example 2 of splitting fields in Section 2, we saw that all three complex roots of $X^3 - X - \frac{1}{3}$ lie in $\mathbb{K}$. Arguing as in Example 1a, we see that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ has order 3, hence that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong C_3$.

Pure Mathematical Physics

(4) $\mathbb{K} = \mathbb{Q}(e^{2\pi i/17})$. According to Section 5, this is the field we need to consider in addressing the constructibility of a regular 17-gon. We saw in that section that $[\mathbb{K} : \mathbb{Q}] = 16$ and that the minimal polynomial of $e^{2\pi i/17}$ over $\mathbb{Q}$ is $X^{16} + X^{15} + \cdots + X + 1$. The other roots of the minimal polynomial in $\mathbb{C}$ are $e^{2\pi il/17}$ for $2 \le l \le 16$, and these all lie in $\mathbb{K}$. Theorem 9.11 therefore gives us a $\mathbb{Q}$ automorphism φ_l of $\mathbb{K}$ sending $e^{2\pi i/17}$ into $e^{2\pi il/17}$ for each l with $1 \le l \le 16$. Since $\mathbb{Q}$ and $e^{2\pi i/17}$ generate $\mathbb{K}$, a $\mathbb{Q}$ automorphism of $\mathbb{K}$ is completely determined by its effect on $e^{2\pi i/17}$. Thus the order of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is 16. Let us determine the group structure. Since φ_l sends $e^{2\pi i/17}$ into $e^{2\pi il/17}$, it sends $e^{2\pi ir/17} = (e^{2\pi i/17})^r$ into $(e^{2\pi il/17})^r = e^{2\pi ilr/17}$. If we drop the exponential from the notation, we can think of φ_l as defined on the integers modulo 17, the formula being $\varphi_l(r) = rl \bmod 17$. From this viewpoint φ_l is an automorphism of the additive group of $\mathbb{F}_{17}$. Lemma 4.45 shows that the group of additive automorphisms of $\mathbb{F}_{17}$ is isomorphic to $\mathbb{F}_{17}^\times$, and it follows from Corollary 4.27 that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong C_{16}$. For our application of constructibility of a regular 17-gon, we would like to know whether the elements of $\mathbb{K}$ are constructible. Taking Theorem 9.24 into account, we therefore seek an intermediate field $\mathbb{L}$ of which $\mathbb{K}$ is a quadratic extension. Since we know that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is cyclic, we can let $H \subseteq \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong C_{16}$ be the 2-element subgroup, and it is natural to try the fixed field $\mathbb{L} = \mathbb{K}^H$. To understand this fixed field, we need to understand the isomorphism $\mathbb{F}_{17}^\times \cong C_{16}$ better. Modulo 17, we have

$$3^2 = 9, \quad 3^4 = -2^2, \quad 3^8 = 2^4 = -1, \quad 3^{16} = 1.$$

Consequently 3 is a generator of the cyclic group $\mathbb{F}_{17}^\times$. Then $H = \{3^8,\ 1\} = \{\pm 1\}$, and $L = \{x \in \mathbb{K} \mid \varphi_{-1}(x) = \varphi_{+1}(x) = x\}$. Since $\varphi_{-1}(e^{2\pi ir/17}) = e^{-2\pi ir/17} = \overline{e^{2\pi ir/17}}$ with the overbar indicating complex conjugation, we see that

$$\mathbb{L} = \mathbb{K}^H = \{x \in \mathbb{K} \mid x = \bar{x}\}.$$

It is not hard to check that indeed $[\mathbb{K} : \mathbb{L}] = 2$. Next we need a subfield $\mathbb{L}'$ of $\mathbb{L}$ with $[\mathbb{L} : \mathbb{L}'] = 2$. We try $\mathbb{L}' = \mathbb{K}^{H'}$ with H' equal to the 4-element cyclic subgroup of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Here we have a harder time checking whether $\mathbb{L}$ is indeed a quadratic extension of $\mathbb{L}'$, but we shall see in Section 8 that it is.[4] We continue in this way, and ultimately we end up with the chain of subfields that exhibits the members of $\mathbb{K}$ as constructible.

We seek to formulate the kind of argument in the above examples as a general theorem. We have to rule out the bad behavior of $\mathbb{Q}(\sqrt[3]{2}\,)$, where one root of the

[4] Actually, Section 8 will point out how Corollary 9.36 in Section 7 already handles this step. In fact, Corollary 9.37 handles this step with no supplementary argument.

Pure Mathematical Physics

minimal polynomial lies in the field but others do not, and we shall do this by assuming that the extension field is a "normal" extension, in a sense to be defined in Section 7. In addition, our style of argument shows that we might run into trouble if our irreducible polynomials over $\Bbbk$ can have repeated roots in $\mathbb{K}$. We shall rule out this bad behavior by insisting that the extension be "separable," a condition that we introduce now. The extension will automatically be separable if $\mathbb{K}$ has characteristic 0.

For the remainder of this section, fix the base field $\Bbbk$. An irreducible polynomial $F(X)$ in $\Bbbk[X]$ is called **separable** if it splits into *distinct* degree-one factors in its splitting field, i.e., if

$$f(X) = a_n(X - x_1)\cdots(X - x_n) \qquad \text{with } x_i \neq x_j \text{ for } i \neq j.$$

Once this splitting into distinct degree-one factors occurs in the splitting field, it occurs in any larger field as well.

Lemma 9.26. A polynomial $F(X)$ in $\Bbbk[X]$ has no repeated roots in its splitting field $\mathbb{K}$ if and only if $\mathrm{GCD}(F, F') = 1$, where $F'(X)$ is the derivative of $F(X)$.

PROOF. The polynomial $F(X)$ has repeated roots in $\mathbb{K}$ if and only if $F(X)$ is divisible by $(X - r)^2$ for some $r \in \mathbb{K}$, if and only if some $r \in \mathbb{K}$ has $F(r) = F'(r) = 0$ (by Corollary 9.17), if and only if some $r \in \mathbb{K}$ has $(X - r)$ dividing $F(X)$ and also $F'(X)$ (by the Factor Theorem), if and only if some $r \in \mathbb{K}$ has $(X - r)$ dividing $\mathrm{GCD}(F, F')$ when the GCD is computed in $\mathbb{K}$, if and only if $\mathrm{GCD}(F, F') \neq 1$ when the GCD is computed in $\mathbb{K}$ (by unique factorization in $\mathbb{K}[X]$). However, the Euclidean algorithm calculates $\mathrm{GCD}(F, F')$ without reference to the field, and the GCD is therefore the same when computed in $\mathbb{K}$ as it is when computed in $\Bbbk$. The lemma follows. □

Proposition 9.27. An irreducible polynomial $F(X)$ in $\Bbbk[X]$ is separable if and only if $F'(X) \neq 0$. In particular, every irreducible (necessarily nonconstant) polynomial is separable if $\Bbbk$ has characteristic 0.

PROOF. Since the polynomial $F(X)$ is irreducible and $\mathrm{GCD}(F, F')$ divides $F(X)$, $\mathrm{GCD}(F, F')$ equals 1 or $F(X)$ in all cases. If $F'(X) = 0$, then $\mathrm{GCD}(F, F') = F(X)$, and Lemma 9.26 implies that $F(X)$ is not separable. Conversely if $F'(X) \neq 0$, then the facts that $\mathrm{GCD}(F, F')$ divides $F'(X)$ and that $\deg F' < \deg F$ together imply that $\mathrm{GCD}(F, F')$ cannot equal $F(X)$. So $\mathrm{GCD}(F, F') = 1$, and Lemma 9.26 implies that $F(X)$ is separable. □

Fix an algebraic extension $\mathbb{K}$ of $\Bbbk$. We say that an element x of $\mathbb{K}$ is **separable** over $\Bbbk$ if the minimal polynomial of x over $\Bbbk$ is separable. We say that $\mathbb{K}$ is a **separable extension** of $\Bbbk$ if every x in $\mathbb{K}$ is separable over $\Bbbk$.

Pure Mathematical Physics

EXAMPLES OF SEPARABLE EXTENSIONS AND EXTENSIONS NOT SEPARABLE.

(1) In characteristic 0, every algebraic extension $\mathbb{K}$ of $\Bbbk$ is separable, by Proposition 9.27.

(2) Every algebraic extension $\mathbb{K}$ of a finite field $\Bbbk$ is separable. In fact, if x is in $\mathbb{K}$, then $[\Bbbk(x) : \Bbbk]$ is finite. Hence $\Bbbk(x)$ is a finite field. Then we may assume that $\mathbb{K}$ is a finite field, say of order $q = p^n$ with p prime. Since the multiplicative group $\mathbb{K}^\times$ has order $q - 1$, every nonzero element of $\mathbb{K}$ is a root of $X^{q-1} - 1$, and every element of $\mathbb{K}$ is therefore a root of $X^q - X$. The minimal polynomial $F(X)$ of x over $\Bbbk$ must then divide $X^q - X$. However, we know that $X^q - X$ splits over $\mathbb{K}$ and has no repeated roots. Thus $F(X)$ splits over $\mathbb{K}$ and has no repeated roots. Then $F(X)$ is separable over $\Bbbk$, and x is separable over $\Bbbk$.

(3) Let $\Bbbk = \mathbb{F}_p(x)$ be a transcendental extension of the finite field $\mathbb{F}_p$. Because this extension is transcendental, $X^p - x$ is irreducible over $\Bbbk$. Let $\mathbb{K}$ be the simple algebraic extension $\Bbbk[X]/(X^p - x)$, which we can write more simply as $\Bbbk(x^{1/p})$. The minimal polynomial of $x^{1/p}$ over $\Bbbk$ is $X^p - x$, and its derivative is $pX^{p-1} = 0$ since the derivative of the constant x is 0. By Proposition 9.27, $x^{1/p}$ is not separable over $\Bbbk$.

The way that separability enters considerations with Galois groups is through the following theorem, explicitly or implicitly. One of the corollaries of the theorem is that if $\mathbb{K}/\Bbbk$ is an algebraic extension, then the set of elements in $\mathbb{K}$ separable over $\Bbbk$ is a subfield of $\mathbb{K}$.

Theorem 9.28. Let $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$ be an inclusion of fields such that $\mathbb{K}$ is a simple algebraic extension of $\mathbb{L}$ of the form $\mathbb{K} = \mathbb{L}(\alpha)$, let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$, and let $M(X)$ be the minimal polynomial of α over $\mathbb{L}$. Then the number of field mappings of $\mathbb{K}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$ is the product of the number of distinct roots of $M(X)$ in $\overline{\mathbb{K}}$ by the number of field mappings of $\mathbb{L}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$.

REMARKS. An algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$ exists by Theorem 9.22. Because $\overline{\mathbb{K}}$ is known to exist, the present theorem reduces to Theorem 9.11 when $\mathbb{L} = \Bbbk$.

PROOF. Any field mapping $\varphi : \mathbb{K} \to \overline{\mathbb{K}}$ is uniquely determined by $\varphi\big|_{\mathbb{L}}$ and $\varphi(\alpha)$. If $\sigma = \varphi\big|_{\mathbb{L}}$, then the equality $M(\alpha) = 0$ implies that $M^\sigma(\varphi(\alpha)) = 0$, and thus $\varphi(\alpha)$ has to be a root of $M^\sigma(X)$. The number of distinct roots of $M^\sigma(X)$ in $\overline{\mathbb{K}}$ equals the number of distinct roots of $M(X)$ in $\overline{\mathbb{K}}$; hence the number of possibilities for $\varphi(\alpha)$ is at most the number of distinct roots of $M(X)$ in $\overline{\mathbb{K}}$. Consequently the number of such φ's fixing $\Bbbk$ is bounded above by the product of the number of distinct roots of $M(X)$ in $\overline{\mathbb{K}}$ times the number of field mappings σ of $\mathbb{L}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$.

For an inequality in the reverse direction, let $\sigma : \mathbb{L} \to \overline{\mathbb{K}}$ be any field mapping of $\mathbb{L}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$, put $\mathbb{L}' = \sigma(\mathbb{L})$, let x be any root of $M^\sigma(X)$, and form the

Pure Mathematical Physics

subfield $\mathbb{L}'(x)$ of $\overline{\mathbb{K}}$. Theorem 9.11′ shows that there exists a field isomorphism $\varphi : \mathbb{L}(\alpha) \to \mathbb{L}'(x)$ with $\varphi\big|_{\mathbb{L}} = \sigma$ and $\varphi(\alpha) = x$, and we can regard φ as a field mapping of $\mathbb{K}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$, extending σ, and having $\varphi(\alpha) = x$. Thus the number of field mappings $\varphi : \mathbb{K} \to \overline{\Bbbk}$ fixing $\Bbbk$ is bounded below by the product of the number of distinct roots of $M(X)$ in $\overline{\mathbb{K}}$ times the number of field homomorphisms σ of $\mathbb{L}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$. □

Corollary 9.29. Let $\mathbb{K} = \Bbbk(\alpha_1, \ldots, \alpha_n)$ be a finite algebraic extension of the field $\Bbbk$, and let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$. Then the number of field mappings of $\mathbb{K}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$ is $\leq [\mathbb{K} : \Bbbk]$. Moreover, the following conditions are equivalent:

(a) the number of field mappings of $\mathbb{K}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$ equals $[\mathbb{K} : \Bbbk]$,
(b) each α_j is separable over $\Bbbk(\alpha_1, \ldots, \alpha_{j-1})$ for $1 \leq j \leq n$,
(c) each α_j is separable over $\Bbbk$ for $1 \leq j \leq n$.

PROOF. The minimal polynomial of α_j over $\Bbbk(\alpha_1, \ldots, \alpha_{j-1})$ divides the minimal polynomial of α_j over $\Bbbk$. If the second of these polynomials has distinct roots in its splitting field, so does the first. Thus (c) implies (b).

For $1 \leq j \leq n$, let the minimal polynomial of α_j over $\Bbbk(\alpha_1, \ldots, \alpha_{j-1})$ be $M_j(X)$, let d_j be the degree of $M_j(X)$, and let s_j be the number of distinct roots of $M_j(X)$ in $\overline{\mathbb{K}}$. Then $s_j \leq d_j$ with equality for a particular j if and only if α_j is separable over $\Bbbk(\alpha_1, \ldots, \alpha_{j-1})$, by definition. Also, $[\mathbb{K} : \Bbbk] = \prod_{j=1}^{n} d_j$ by Corollary 9.7, and the number of field mappings of $\mathbb{K}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$ is $\prod_{j=1}^{n} s_j$ by iterated application of Theorem 9.28. From these facts, the first conclusion of the corollary is immediate, and so is the equivalence of (a) and (b).

Condition (a) is independent of the order of enumeration of $\alpha_1, \ldots, \alpha_n$. Since we can always take any particular α_j to be first, we see that (a) implies (c). □

Corollary 9.30. Let $\mathbb{K} = \Bbbk(\alpha_1, \ldots, \alpha_n)$ be a finite algebraic extension of the field $\Bbbk$. If each α_j for $1 \leq j \leq n$ is separable over $\Bbbk$, then $\mathbb{K}/\Bbbk$ is a separable extension.

PROOF. Let β be in $\mathbb{K}$, We apply the equivalence of (a) and (c) in Corollary 9.29 once to the set of generators $\{\alpha_1, \ldots, \alpha_n\}$ and once to the set of generators $\{\beta, \alpha_1, \ldots, \alpha_n\}$, and the result is immediate. □

Corollary 9.31. If $\mathbb{K}/\Bbbk$ is an algebraic field extension, then the subset $\mathbb{L}$ of elements of $\mathbb{K}$ that are separable over $\Bbbk$ is a subfield of $\mathbb{K}$.

PROOF. If α and β are given in $\mathbb{L}$, we apply Corollary 9.30 to the extension $\Bbbk(\alpha, \beta)$ of $\Bbbk$ to see that $\mathbb{L}$ contains the subfield generated by $\Bbbk$ and the elements α and β. □

Proposition 9.32. If $\mathbb{K}/\Bbbk$ is a separable algebraic extension and if $\mathbb{L}$ is a field with $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$, then $\mathbb{K}$ is separable over $\mathbb{L}$, and $\mathbb{L}$ is separable over $\Bbbk$.

PROOF. The separability assertion about $\mathbb{L}/\Bbbk$ says the same thing about elements of $\mathbb{L}$ that separability of $\mathbb{K}/\Bbbk$ says about those same elements, and it is therefore immediate that $\mathbb{L}/\Bbbk$ is separable.

Next let us consider $\mathbb{K}/\mathbb{L}$. If x is in $\mathbb{K}$, let $F(X)$ be its minimal polynomial over $\Bbbk$, and let $G(X)$ be its minimal polynomial over $\mathbb{L}$. Since $F(X)$ is in $\mathbb{L}[X]$ and $F(x) = G(x) = 0$, $G(X)$ divides $F(X)$. Since $\mathbb{K}/\Bbbk$ is separable, $F(X)$ splits into distinct degree-one factors in its splitting field $\mathbb{F}$. The field $\mathbb{F}$ contains the splitting field of $G(X)$, and thus the degree-one factors of $G(X)$ in $\mathbb{F}[X]$ are a subset of the degree-one factors of $F(X)$ in $\mathbb{F}[X]$. There are no repeated factors for $F(X)$, and there can be no repeated factors for $G(X)$. Thus x is separable over $\mathbb{L}$, and $\mathbb{K}/\mathbb{L}$ is a separable extension. □

In studying Galois groups, we shall be chiefly interested in the following situation in Corollary 9.29: $\mathbb{K}$ is an algebraic field extension $\mathbb{K} = \Bbbk(\alpha_1, \ldots, \alpha_n)$ of $\Bbbk$ for which every field mapping of $\mathbb{K}$ into an algebraic closure that fixes $\Bbbk$ actually carries $\mathbb{K}$ into itself. We seek conditions under which this situation arises, and then we mine the consequences. As we did in the study begun in Theorem 9.28, we begin with the case of a simple algebraic extension.

Let $\mathbb{K} = \Bbbk(\gamma)$ be a simple algebraic extension of $\Bbbk$, and let $F(X)$ be the minimal polynomial of γ over $\Bbbk$. Any member φ of the Galois group $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ carries γ to another root γ' of $F(X)$, and φ is uniquely determined by γ' since $\Bbbk$ and γ generate the field $\mathbb{K}$. An element φ of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ carrying γ to γ' can exist only if γ' is in $\mathbb{K}$. If γ' is in $\mathbb{K}$, then $\Bbbk(\gamma) \supseteq \Bbbk(\gamma')$, and the equal finite dimensionality of $\Bbbk(\gamma)$ and $\Bbbk(\gamma')$ forces $\Bbbk(\gamma) = \Bbbk(\gamma')$. In other words, if γ' is in $\mathbb{K}$, then the unique $\Bbbk$ isomorphism $\Bbbk(\gamma) \to \Bbbk(\gamma')$ of Theorems 9.10 and 9.11 carrying γ to γ' is a member of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. Making a count of what happens to all the elements γ', we see that we have proved the following.

Proposition 9.33. Let $\mathbb{K} = \Bbbk(\gamma)$ be a simple algebraic extension of $\Bbbk$, and let $F(X)$ be the minimal polynomial of γ. Then

$$|\mathrm{Gal}(\mathbb{K}/\Bbbk)| \leq [\mathbb{K} : \Bbbk]$$

with equality if and only if $F(X)$ is a separable polynomial and $\mathbb{K}$ is the splitting field of $F(X)$ over $\Bbbk$.

EXAMPLE. For $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$ with minimal polynomial $F(X)$, we know that $F(X)$ does not split in $\mathbb{K}$; the nonreal roots of $F(X)$ do not lie in $\mathbb{K}$. Proposition 9.33 gives us $|\mathrm{Gal}(\mathbb{K}/\mathbb{Q})| < [\mathbb{K} : \mathbb{Q}] = 3$, and a glance at the argument preceding Proposition 9.33 shows that $|\mathrm{Gal}(\mathbb{K}/\mathbb{Q})|$ has to be 1.

Pure Mathematical Physics

It is possible to investigate the case of several generators directly, but it is more illuminating to reduce it to the case of a single generator as in Proposition 9.33. The tool for doing so is the following important theorem.

Theorem 9.34 (Theorem of the Primitive Element). Let $\mathbb{K}/\Bbbk$ be a separable algebraic extension with $[\mathbb{K} : \Bbbk] < \infty$. Then there exists an element γ in $\mathbb{K}$ such that $\mathbb{K} = \Bbbk(\gamma)$.

PROOF. We may assume that $\Bbbk$ is infinite because Corollary 4.27 shows that the multiplicative group of a finite field is cyclic. With $\Bbbk$ infinite, we can write $\mathbb{K} = \Bbbk(x_1, \ldots, x_n)$, and we proceed by induction on n, the case $n = 1$ being trivial. For general n, let $\mathbb{L} = \Bbbk(x_1, \ldots, x_{n-1})$, so that $\mathbb{K} = \mathbb{L}(x_n)$. By the inductive hypothesis, $\mathbb{L}$ is of the form $\mathbb{L} = \Bbbk(\alpha)$ for some α in $\mathbb{K}$, and thus $\mathbb{K} = \Bbbk(\alpha, x_n)$. Changing notation, we see that it is enough to prove that whenever $\mathbb{K}$ is a separable algebraic extension of the form $\mathbb{K} = \Bbbk(\alpha, \beta)$, then $\mathbb{K}$ is of the form $\mathbb{K} = \Bbbk(\gamma)$ for some γ. We shall show this for γ of the form $\gamma = \beta + c\alpha$ for some c in $\Bbbk$.

Let $F(X)$ and $G(X)$ be the minimal polynomials of α and β over $\Bbbk$, and let $\mathbb{K}'$ be an extension in which $F(X)G(X)$ splits, i.e., in which $F(X)$ and $G(X)$ both split. Let $\alpha_1 = \alpha,\ \alpha_2, \ldots, \alpha_m$ and $\beta_1 = \beta,\ \beta_2, \ldots, \beta_n$ be the roots of $F(X)$ and $G(X)$ in $\mathbb{K}'$, In each case the roots are necessarily distinct by definition of separability of α and β. Define $\mathbb{L} = \Bbbk(\gamma)$ with $\gamma = \beta + c\alpha$, where c is a member of $\Bbbk$ yet to be specified. For suitable c, we shall show that α is in $\mathbb{L}$. Then $\beta = \gamma - c\alpha$ must be in $\mathbb{L}$, and we obtain $\mathbb{K} \subseteq \mathbb{L}$. Since γ is in $\mathbb{K}$, the reverse inclusion is built into the construction, and thus we will have $\mathbb{K} = \mathbb{L}$.

We shall compute the minimal polynomial of α over $\mathbb{L}$. We know that α is a root of $F(X)$, and we put $H(X) = G(\gamma - cX)$. Then $H(X)$ is in $\mathbb{L}[X] \subseteq \mathbb{K}'[X]$, and $G(\beta) = 0$ implies $H(\alpha) = 0$. Therefore $X - \alpha$ divides both $F(X)$ and $H(X)$ in the ring $\mathbb{K}'[X]$. Let us determine $\mathrm{GCD}(F, H)$ in $\mathbb{K}'[X]$. The separability of α says that $X - \alpha$ divides $F(X)$ only once. Since $F(X)$ splits in $\mathbb{K}'[x]$, any other prime divisor of $\mathrm{GCD}(F, H)$ in $\mathbb{K}'[X]$ has to be of the form $X - \alpha_i$ with $i \neq 1$. The definition of $H(X)$ gives $H(\alpha_i) = G(\gamma - c\alpha_i)$. If $G(\gamma - c\alpha_i) = 0$, then $\gamma - c\alpha_i = \beta_j$ for some j, with the consequence that $\beta + c\alpha - c\alpha_i = \beta_j$ and $c = (\beta_j - \beta)(\alpha - \alpha_i)^{-1}$. Since $\Bbbk$ is an infinite field, we can choose c in $\mathbb{K}$ different from all the finitely many quotients $(\beta_j - \beta)(\alpha - \alpha_i)^{-1}$. For such a choice of c, $\mathrm{GCD}(F, H) = X - \alpha$ in $\mathbb{K}'[X]$. Then $\mathrm{GCD}(F, H) = X - \alpha$, up to a scalar factor, in $\mathbb{L}[X]$ since $F(X)$ and $H(X)$ are in $\mathbb{L}[X]$ and since the GCD can be computed without reference to the field containing both elements. The ratio of the constant term to the coefficient of X has to be in $\mathbb{L}$ independently of the scalar factor multiplying $X - \alpha$, and therefore α is in $\mathbb{L}$. This completes the proof. □

7. Normal Extensions

In using Galois groups to help in understanding field extensions, an example to keep in mind is the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. In this case the Galois group is trivial and therefore gives us no information about the extension. Thus it makes sense to regard the failure of equality to hold in an inequality $|\operatorname{Gal}(\mathbb{K}/\Bbbk)| \le [\mathbb{K} : \Bbbk]$ as an undesirable situation.[5]

Proposition 9.33 suggests that the failure of equality to hold in the inequality $|\operatorname{Gal}(\mathbb{K}/\Bbbk)| \le [\mathbb{K} : \Bbbk]$ has something to do with two phenomena. One is the possible failure of some polynomials over $\Bbbk$ to be separable, and the other is the failure of polynomials over $\Bbbk$ to split fully in $\mathbb{K}$ once they have at least one root in $\mathbb{K}$. Having examined separability in Section 6, we turn to this question of full splitting of polynomials.

Accordingly, we make a definition, choosing among several equivalent conditions the one that is usually the easiest to check in practice. A finite[6] algebraic extension $\mathbb{K}$ of a field $\Bbbk$ is said to be **normal** over $\Bbbk$ if $\mathbb{K}$ is the splitting field of *some* $F(X)$ in $\Bbbk[X]$. The following proposition gives some equivalent formulations of this condition.

Proposition 9.34A. Let $\mathbb{K}$ be a finite algebraic extension of a field $\Bbbk$, and regard $\mathbb{K}$ as contained in a fixed algebraic closure $\overline{\mathbb{K}}$. Then the following conditions on $\mathbb{K}$ are equivalent.

(a) $\mathbb{K}$ is the splitting field of *some* $F(X)$ in $\Bbbk[X]$, i.e., $\mathbb{K}$ is normal over $\Bbbk$,
(b) *every* irreducible polynomial $M(X)$ in $\Bbbk[X]$ with a root in $\mathbb{K}$ splits in $\mathbb{K}$, i.e., $\mathbb{K}$ contains the splitting field for each such $M(X)$,
(c) every $\Bbbk$ isomorphism of $\mathbb{K}$ into $\overline{\mathbb{K}}$ carries $\mathbb{K}$ into itself.

REMARK. Although (a) is often the easiest of the conditions to check, (b) is often the easiest to disprove. It is therefore quite handy to know the equivalence.

PROOF. Suppose that (a) holds. Let $F(X)$ be as in (a), and let its roots be $\gamma_1, \dots, \gamma_n$. Let $M(X)$ be an irreducible polynomial in $\Bbbk[X]$ with a root α in $\mathbb{K}$, and let $\mathbb{L}$ be the splitting field of $M(X)$ over $\mathbb{K}$. Let β be any root of $M(X)$ in $\mathbb{L}$. Since $M(X)$ is irreducible over $\Bbbk$, Theorem 9.11 produces a $\Bbbk$ isomorphism σ of $\Bbbk(\alpha)$ onto $\Bbbk(\beta)$ with $\sigma(\alpha) = \beta$. The isomorphism σ leaves $F(X)$ fixed, since the coefficients of $F(X)$ are in $\Bbbk$. Now the splitting field of $F(X)$ over $\Bbbk(\alpha)$

[5] We obtained this inequality in Proposition 9.33 only when $\mathbb{K}$ has a single generator over $\Bbbk$, but we take this case as indicative of what to expect more generally.

[6] Many books do not restrict the definition to finite extensions. The additional generality of infinite algebraic extensions will not be of benefit for our current purposes, and thus we restrict to finite extensions for now. But in Section VII.6 of *Advanced Algebra*, we shall enlarge the definition of "normal" to allow infinite algebraic extensions.

is $\mathbb{K}$, since the roots of $F(X)$ are in $\mathbb{K}$ and generate $\mathbb{K}$ over $\Bbbk(\alpha)$. Similarly the splitting field of $F(X)$ over $\Bbbk(\beta)$ is $\mathbb{K}(\beta)$. Application of Theorem 9.13′ yields a field isomorphism φ of $\mathbb{K}$ onto $\mathbb{K}(\beta)$ such that $\varphi\big|_{\Bbbk(\alpha)} = \sigma$ and such that φ carries the roots of $F(X)$ to the roots of $F(X)$. We can express α as a rational expression in $\gamma_1, \ldots, \gamma_n$ with coefficients in $\Bbbk$, and then $\beta = \varphi(\alpha)$ is the same rational expression in $\varphi(\gamma_1), \ldots, \varphi(\gamma_n)$, which themselves are members of $\mathbb{K}$. Therefore β is in $\mathbb{K}$, and the conclusion is that $M(X)$ splits in $\mathbb{K}$.

Suppose that (b) holds. Let φ be a $\Bbbk$ isomorphism of $\mathbb{K}$ into $\overline{\mathbb{K}}$, and let α be any element of $\mathbb{K}$. The minimal polynomial $M(X)$ of α over $\Bbbk$ is irreducible and has α as a root in $\mathbb{K}$. By (b), $M(X)$ splits in $\mathbb{K}$. The element $\varphi(\alpha)$ has to be a root of $M(X)$ since φ fixes the coefficients of $M(X)$, and all the roots of $M(X)$ are assumed to lie in $\mathbb{K}$. Therefore $\varphi(\alpha)$ lies in $\mathbb{K}$, and (b) implies (c).

Suppose that (c) holds. Since $\mathbb{K}$ is a finite algebraic extension of $\Bbbk$, we can write $\mathbb{K} = \Bbbk(\alpha_1, \ldots, \alpha_n)$ for suitable elements $\alpha_1, \ldots, \alpha_n$ of $\mathbb{K}$. Let $P_j(X)$ be the minimal polynomial of α_j over $\Bbbk$, and put $F(X) = \prod_{j=1}^{n} P_j(X)$. Since the roots $\alpha_1, \ldots, \alpha_n$ generate $\mathbb{K}$ over $\Bbbk$, it is enough to show that every root of $F(X)$ lies in K, i.e., each root of each $P_j(X)$ lies in $\mathbb{K}$. Let β be a root of $P_j(X)$ in $\overline{\mathbb{K}}$. We know from Theorem 9.11 that there is a $\Bbbk$ isomorphism φ of $\Bbbk(\alpha_j)$ onto $\Bbbk(\beta)$ with $\varphi(\alpha_j) = \beta$. Theorem 9.23 shows that φ extends to a field mapping of $\mathbb{K}$ into $\overline{\mathbb{K}}$, and (c) shows that the extended φ sends $\mathbb{K}$ into itself. Therefore $\beta = \varphi(\alpha_j)$ lies in $\mathbb{K}$, and all the roots of $F(X)$ in $\overline{\mathbb{K}}$ lie in $\mathbb{K}$. Thus (c) implies (a). □

Now we can put together the properties of normal and separable extensions. It will be convenient to be able to refer in this context to the equivalence of (a) and (b) that was proved in Proposition 9.34A, and thus we repeat the statement of that equivalence here.

Proposition 9.35. Let $\mathbb{K}$ be a finite separable algebraic extension of a field $\Bbbk$, so that $|\operatorname{Gal}(\mathbb{K}/\Bbbk)| \le [\mathbb{K} : \Bbbk]$. Then the following are equivalent.

(a) $\mathbb{K}$ is the splitting field of *some* $F(X)$ in $\Bbbk[X]$, i.e., $\mathbb{K}$ is normal over $\Bbbk$,
(b) *every* irreducible polynomial $M(X)$ in $\Bbbk[X]$ with a root in $\mathbb{K}$ splits in $\mathbb{K}$, i.e., $\mathbb{K}$ contains the splitting field for each such $M(X)$,
(c) $|\operatorname{Gal}(\mathbb{K}/\Bbbk)| = [\mathbb{K} : \Bbbk]$,
(d) $\Bbbk = \mathbb{K}^G$ for $G = \operatorname{Gal}(\mathbb{K}/\Bbbk)$.

REMARKS. The equivalence of (a) and (b) is part of Proposition 9.34A, and the fact that they are equivalent with (c) follows from Proposition 9.33 and the Theorem of the Primitive Element (Theorem 9.34). We prove that the equivalent (a), (b), and (c) imply (d), and that (d) implies (b).

PROOF. Suppose that the equivalent (a), (b), and (c) hold for $\mathbb{K}/\Bbbk$. We prove (d). Write $G = \operatorname{Gal}(\mathbb{K}/\Bbbk)$, and let $\Bbbk' = \mathbb{K}^G$. Since every member of $\operatorname{Gal}(\mathbb{K}/\Bbbk)$

Pure Mathematical Physics

fixes $\Bbbk'$, $\mathrm{Gal}(\mathbb{K}/\Bbbk) \subseteq \mathrm{Gal}(\mathbb{K}/\Bbbk')$. Meanwhile, (a) for $\mathbb{K}/\Bbbk$ implies (a) for $\mathbb{K}/\Bbbk'$, and $\mathbb{K}$ is separable over $\Bbbk'$ by Proposition 9.32. Since (a) implies (c), (c) holds for both $\Bbbk'$ and $\Bbbk$, and we have

$$[\mathbb{K} : \Bbbk] = |\,\mathrm{Gal}(\mathbb{K}/\Bbbk)| \le |\,\mathrm{Gal}(\mathbb{K}/\Bbbk')| = [\mathbb{K} : \Bbbk'].$$

Since $\Bbbk' \supseteq \Bbbk$, the inequality of dimensions implies that $\Bbbk' = \Bbbk$. Thus (d) holds.

Suppose (d) holds. We prove (b). Let $M(X)$ be an irreducible polynomial in $\Bbbk[X]$ having a root r in $\mathbb{K}$. The polynomial $M(X)$ is necessarily the minimal polynomial of r over $\Bbbk$. Define

$$J(X) = \prod_{\varphi \in G} (X - \varphi(r)). \tag{$*$}$$

If φ_0 is in G, then F^{φ_0} is given by replacing each $\varphi(x)$ by $\varphi_0\varphi(r)$, and the product is unchanged. Therefore $J(X) = J^{\varphi_0}(X)$, and $J(X)$ is in $\mathbb{K}^G[X]$. From the assumption in (d), $\mathbb{K}^G = \Bbbk$. Therefore $J(X)$ is in $\Bbbk[X]$. Since $J(r) = 0$ and since $M(X)$ is the minimal polynomial of r over $\Bbbk$, $M(X)$ divides $J(X)$. Over $\mathbb{K}$, $J(X)$ splits because of its definition in $(*)$. By unique factorization in $\mathbb{K}[X]$, $M(X)$ must split too. Thus $M(X)$ splits in $\mathbb{K}[X]$, and (b) holds. □

Corollary 9.36. If $\mathbb{K}$ is a finite normal separable extension of $\Bbbk$ and if $\mathbb{L}$ is a field with $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$, then $\mathbb{K}$ is a finite normal separable extension of $\mathbb{L}$, and the subgroup $H = \mathrm{Gal}(\mathbb{K}/\mathbb{L})$ of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ has

$$\boxed{|H| \cdot [\mathbb{L} : \Bbbk] = |\,\mathrm{Gal}(\mathbb{K}/\Bbbk)|\,.}$$

PROOF. The field $\mathbb{K}$ is a separable extension of the intermediate field $\mathbb{L}$ by Proposition 9.32, and it is a normal extension by Proposition 9.35a. Therefore Proposition 9.35c gives $|\,\mathrm{Gal}(\mathbb{K}/\mathbb{L})| = [\mathbb{K} : \mathbb{L}]$, and we have

$$|H| \cdot [\mathbb{L} : \Bbbk] = |\,\mathrm{Gal}(\mathbb{K}/\mathbb{L})| \cdot [\mathbb{L} : \Bbbk] = [\mathbb{K} : \mathbb{L}] \cdot [\mathbb{L} : \Bbbk] = [\mathbb{K} : \Bbbk] = |\,\mathrm{Gal}(\mathbb{K}/\Bbbk)|,$$

the last two equalities holding by Corollary 9.7 and Proposition 9.35c. □

Corollary 9.37. Let $\mathbb{K}/\Bbbk$ be a separable algebraic extension, and suppose that H is a finite subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. Then $\mathbb{K}/\mathbb{K}^H$ is a finite normal separable extension, H is the subgroup $\mathrm{Gal}(\mathbb{K}/\mathbb{K}^H)$ of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, and $[\mathbb{K} : \mathbb{K}^H] = |H|$.

PROOF. Proposition 9.32 shows that $\mathbb{K}$ is separable over $\mathbb{K}^H$. For an arbitrary element x of $\mathbb{K}$, form the polynomial in $\mathbb{K}[X]$ given by

$$F(X) = \prod_{\varphi \in H} (X - \varphi(x)).$$

Pure Mathematical Physics

If φ_0 is in H, then F^{φ_0} is given by replacing each $\varphi(x)$ by $\varphi_0\varphi(x)$, and the product is unchanged. Therefore $F(X) = F^{\varphi_0}(X)$, and $F(X)$ is in $\mathbb{K}^H[X]$. Thus $F(X)$ is a polynomial in $\mathbb{K}^H[X]$ that has x as a root and splits in $\mathbb{K}$. The minimal polynomial $M(X)$ of x over $\mathbb{K}^H$ must divide $F(X)$, and it too has x as a root. By unique factorization in $\mathbb{K}[X]$, $M(X)$ must split in $\mathbb{K}$. Thus $\mathbb{K}/\mathbb{K}^H$ will be a normal extension if it is shown that $[\mathbb{K} : \mathbb{K}^H] < \infty$.

The element x has $[\mathbb{K}^H(x) : \mathbb{K}^H] = \deg M(X) \le \deg F(X) = |H|$, and the claim is that $[\mathbb{K} : \mathbb{K}^H] \le |H|$. Assuming the contrary, we would at some point have an inequality $[\mathbb{K}^H(x_1, \dots, x_n) : \mathbb{K}^H] > |H|$ because every element of $\mathbb{K}$ is algebraic over $\Bbbk$. By the Theorem of the Primitive Element (Theorem 9.34), $\mathbb{K}^H(x_1, \dots, x_n) = \mathbb{K}^H(z)$ for some element z, and therefore $[\mathbb{K}^H(x_1, \dots, x_n) : \mathbb{K}^H] = [\mathbb{K}^H(z) : \mathbb{K}^H] \le |H|$, contradiction. We conclude that $[\mathbb{K} : \mathbb{K}^H] \le |H|$. From the previous paragraph, $\mathbb{K}/\mathbb{K}^H$ is a finite separable normal extension.

The definition of $\mathbb{K}^H$ shows that $H \subseteq \mathrm{Gal}(\mathbb{K}/\mathbb{K}^H)$, and Proposition 9.35c gives $|\mathrm{Gal}(\mathbb{K}/\mathbb{K}^H)| = [\mathbb{K} : \mathbb{K}^H]$. Putting these facts together with the inequality $[\mathbb{K} : \mathbb{K}^H] \le |H|$ from the previous paragraph, we have

$$|H| \le |\mathrm{Gal}(\mathbb{K}/\mathbb{K}^H)| = [\mathbb{K} : \mathbb{K}^H] \le |H|$$

with equality on the left only if $H = \mathrm{Gal}(\mathbb{K}/\mathbb{K}^H)$. Equality must hold throughout the displayed line since the ends are equal, and therefore $H = \mathrm{Gal}(\mathbb{K}/\mathbb{K}^H)$. □

8. Fundamental Theorem of Galois Theory

We are now in a position to obtain the main result in Galois theory.

Theorem 9.38 (Fundamental Theorem of Galois Theory). If $\mathbb{K}$ is a finite normal separable extension of $\Bbbk$, then there is a one-one inclusion-reversing correspondence between the subgroups H of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ and the subfields $\mathbb{L}$ of $\mathbb{K}$ that contain $\Bbbk$, corresponding elements H and $\mathbb{L}$ being given by

$$\mathbb{L} = \mathbb{K}^H \qquad \text{and} \qquad H = \mathrm{Gal}(\mathbb{K}/\mathbb{L}).$$

The effect of the theorem is to take an extremely difficult problem, namely finding intermediate fields, and reduce it to a problem that is merely difficult, namely finding the Galois group. For example the finiteness of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ implies that there are only finitely many subgroups of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, and the theorem therefore implies that there are only finitely many intermediate fields; this finiteness of the number of intermediate fields is not so obvious without the theorem.

As a reminder of the availability of Theorem 9.38, Proposition 9.35, and Corollary 9.36, it is customary to refer to a finite normal separable extension as a **finite Galois extension**.

Before coming to the proof of the theorem, let us examine what the theorem says for the examples in Section 6. In each case the field $\Bbbk$ is the field $\mathbb{Q}$ of rationals. The extensions are separable because the characteristic is 0.

EXAMPLES.

(1a) $\mathbb{K} = \mathbb{Q}(\sqrt{-1}\,)$. This is the splitting field[7] for $X^2 + 1$. Proposition 9.33 gives $|\operatorname{Gal}(\mathbb{K}/\mathbb{Q})| = [\mathbb{K} : \mathbb{Q}] = 2$. Thus $\operatorname{Gal}(\mathbb{K}/\mathbb{Q}) \cong C_2$. There are no nontrivial subgroups, and there are consequently no intermediate fields. We knew this already since there cannot be any intermediate $\mathbb{Q}$ vector spaces between $\mathbb{Q}$ and $\mathbb{K}$. Thus the theorem tells us nothing new.

(1b) $\mathbb{K} = \mathbb{Q}(\sqrt{2}\,)$. Similar remarks apply.

(2) $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}\,)$. This extension is not normal, as a consequence of (b) in Proposition 9.34A. (Namely $X^3 - 2$ has a root in $\mathbb{K}$ but does not split in $\mathbb{K}$.) Theorem 9.38 does not apply to $\mathbb{K}$. If we adjoin r to $\mathbb{K}$ with $r^2 + (\sqrt[3]{2}\,)r + (\sqrt[3]{2}\,)^2 = 0$, we obtain the splitting field $\mathbb{K}'$ for $X^3 - 2$ over $\mathbb{Q}$. Then $\mathbb{K}'$ is a normal extension of $\mathbb{Q}$, and the theorem applies. Since each element of $\operatorname{Gal}(\mathbb{K}'/\mathbb{Q})$ permutes the three roots of $X^3 - 2$ and is determined by its effect on these roots, $\operatorname{Gal}(\mathbb{K}'/\mathbb{Q})$ is isomorphic to a subgroup of the symmetric group $\mathfrak{S}_3$. The Galois group $\operatorname{Gal}(\mathbb{K}'/\mathbb{Q})$ has order $[\mathbb{K}' : \mathbb{Q}] = 6$ and hence is isomorphic to the whole symmetric group $\mathfrak{S}_3$. The group $\mathfrak{S}_3$ has three subgroups of order 2 and one subgroup of order 3. Therefore $\mathbb{K}'$ has three intermediate fields of degree 3 and one of degree 2. The intermediate fields of degree 3 are the three fields generated by $\mathbb{Q}$ and one of the three roots of $X^3 - 2$. The intermediate field of degree 2 corresponds to the alternating subgroup of order 3 and is the subfield generated by $\mathbb{Q}$ and the cube roots of 1. It is the splitting field for $X^2 + X + 1$ over $\mathbb{Q}$.

(3) $\mathbb{K} = \mathbb{Q}(r)$, where r is a root of $X^3 - X - \frac{1}{3}$. We know from Section 2 that $X^3 - X - \frac{1}{3}$ is irreducible over $\mathbb{Q}$ and splits in $\mathbb{K}$, and $\mathbb{K}$ by definition is therefore normal. Proposition 9.33 tells us that $\operatorname{Gal}(\mathbb{K}/\mathbb{Q})$ has order 3 and hence is isomorphic to C_3. There are no nontrivial subgroups, and Theorem 9.38 tells us that there are no intermediate fields. We could have seen in more elementary fashion that there are no intermediate fields by using Corollary 9.7, since the corollary tells us that the degree of an intermediate field would have to divide 3.

(4) $\mathbb{K} = \mathbb{Q}(e^{2\pi\, 1/17})$. We have seen that $[\mathbb{K} : \mathbb{Q}] = 16$ and that $\operatorname{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{F}_{17}^{\times} \cong C_{16}$. Let c be a generator of the cyclic Galois group. Let $H_2 = \{1, c^8\}$,

[7] It is customary to regard the algebraic closure of $\mathbb{Q}$ as a subfield of $\mathbb{C}$, and thus there is no ambiguity in referring to *the* splitting field.

Pure Mathematical Physics

$H_4 = \{1, c^4, c^8, c^{12}\}$, and $H_8 = \{1, c^2, c^4, c^6, c^8, c^{10}, c^{12}, c^{14}\}$. Then put

$$\mathbb{L}_2 = \mathbb{K}^{H_2}, \qquad \mathbb{L}_4 = \mathbb{K}^{H_4}, \qquad \mathbb{L}_8 = \mathbb{K}^{H_8}.$$

The inclusions among our subgroups are

$$\{1\} \subseteq H_2 \subseteq H_4 \subseteq H_8 \subseteq \mathrm{Gal}(\mathbb{K}/\mathbb{Q}),$$

and the theorem says that the correspondence with intermediate fields reverses inclusions. Then we have

$$\mathbb{K} \supseteq \mathbb{L}_2 \supseteq \mathbb{L}_4 \supseteq \mathbb{L}_8 \supseteq \mathbb{Q}.$$

Applying Corollary 9.36, we see that each of these subfields is a quadratic extension of the next-smaller one. Theorem 9.24 says that the members of $\mathbb{K}$ are therefore constructible with straightedge and compass. Consequently a regular 17-gon is constructible with straightedge and compass. The constructibility or nonconstructibility of regular n-gons for general n will be settled in similar fashion in the next section. In Section 12 we return to the question of using Galois theory to guide us through the actual steps of the construction when it is possible.

PROOF OF THEOREM 9.38. The function $\mathbb{L} \mapsto \mathrm{Gal}(\mathbb{K}/\mathbb{L})$ has domain the set of all intermediate fields and range the set of all subgroups of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, since an element in $\mathrm{Gal}(\mathbb{K}/\mathbb{L})$ is necessarily in $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. Each such extension $\mathbb{K}/\mathbb{L}$ is separable by Proposition 9.32 and is normal by Proposition 9.34A. Thus Proposition 9.35d applies to each $\mathbb{K}/\mathbb{L}$ and shows that $\mathbb{L} = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{L})}$. Consequently the function $\mathbb{L} \mapsto \mathrm{Gal}(\mathbb{K}/\mathbb{L})$ is one-one. If H is a subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, then Corollary 9.37 shows that $\mathbb{L} = \mathbb{K}^H$ is an intermediate field for which $H = \mathrm{Gal}(\mathbb{K}/\mathbb{L})$, and therefore the function $\mathbb{L} \mapsto \mathrm{Gal}(\mathbb{K}/\mathbb{L})$ is onto.

It is immediate from the definition of Galois group that $\mathbb{L}_1 \subseteq \mathbb{L}_2$ implies $\mathrm{Gal}(\mathbb{K}/\mathbb{L}_1) \supseteq \mathrm{Gal}(\mathbb{K}/\mathbb{L}_2)$, and it is immediate from the formula $\mathbb{L} = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{L})}$ that $\mathrm{Gal}(\mathbb{K}/\mathbb{L}_1) \supseteq \mathrm{Gal}(\mathbb{K}/\mathbb{L}_2)$ implies $\mathbb{L}_1 \subseteq \mathbb{L}_2$. This completes the proof. □

Corollary 9.39. If $\mathbb{K}$ is a finite Galois extension of $\Bbbk$ and if $\mathbb{L}$ is a subfield of $\mathbb{K}$ that contains $\Bbbk$, then $\mathbb{L}$ is a normal extension of $\Bbbk$ if and only if $\mathrm{Gal}(\mathbb{K}/\mathbb{L})$ is a normal subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. In this case, the map $\mathrm{Gal}(\mathbb{K}/\Bbbk) \to \mathrm{Gal}(\mathbb{L}/\Bbbk)$ given by restriction from $\mathbb{K}$ to $\mathbb{L}$ is a group homomorphism that descends to a group isomorphism

$$\mathrm{Gal}(\mathbb{K}/\Bbbk) \big/ \mathrm{Gal}(\mathbb{K}/\mathbb{L}) \cong \mathrm{Gal}(\mathbb{L}/\Bbbk).$$

Pure Mathematical Physics

PROOF. Let $\mathbb{L}$ correspond to $H = \mathrm{Gal}(\mathbb{K}/\mathbb{L})$ in Theorem 9.38, so that $\mathbb{L} = \mathbb{K}^H$. If φ is in $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, then

$$\begin{aligned}\mathbb{K}^{\varphi H \varphi^{-1}} &= \{k \in \mathbb{K} \mid \varphi h \varphi^{-1}(k) = k \text{ for all } h \in H\} \\ &= \{\varphi(k') \in \mathbb{K} \mid \varphi h(k') = \varphi(k') \text{ for all } h \in H\} \\ &= \{\varphi(k') \in \mathbb{K} \mid h(k') = k' \text{ for all } h \in H\} \\ &= \varphi(\mathbb{K}^H) = \varphi(\mathbb{L}).\end{aligned}$$

Since the correspondence of Theorem 9.38 is one-one onto, $\varphi H \varphi^{-1} = H$ if and only if $\varphi(\mathbb{L}) = \mathbb{L}$. Therefore H is a normal subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ if and only if $\varphi(\mathbb{L}) = \mathbb{L}$ for all $\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk)$.

Now suppose that H is a normal subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. We have just seen that $\varphi(\mathbb{L}) = \mathbb{L}$ for all $\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk)$. Then each φ defines by restriction a member $\overline{\varphi} = \varphi\big|_{\mathbb{L}}$ of $\mathrm{Gal}(\mathbb{L}/\Bbbk)$, and $\varphi \mapsto \overline{\varphi}$ is certainly a group homomorphism. The kernel of $\varphi \mapsto \overline{\varphi}$ is the subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ given by

$$\left\{\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk) \;\middle|\; \varphi\big|_{\mathbb{L}} = 1\right\},$$

and this is just $\mathrm{Gal}(\mathbb{K}/\mathbb{L})$. Thus $\varphi \mapsto \overline{\varphi}$ descends to a one-one homomorphism of $\mathrm{Gal}(\mathbb{K}/\Bbbk)\big/\mathrm{Gal}(\mathbb{K}/\mathbb{L})$ into $\mathrm{Gal}(\mathbb{L}/\Bbbk)$, and we have

$$|\mathrm{Gal}(\mathbb{K}/\Bbbk)|/|\mathrm{Gal}(\mathbb{K}/\mathbb{L})| \le |\mathrm{Gal}(\mathbb{L}/\Bbbk)|.$$

We make use of Corollary 9.7 relating degrees of extensions. Applying Proposition 9.35c to $\mathbb{K}/\Bbbk$ and $\mathbb{K}/\mathbb{L}$, as well as Proposition 9.33 to $\mathbb{L}/\Bbbk$, we obtain

$$\begin{aligned}[\mathbb{L} : \Bbbk] &= [\mathbb{K} : \Bbbk]\big/[\mathbb{K} : \mathbb{L}] \\ &= |\mathrm{Gal}(\mathbb{K}/\Bbbk)|/|\mathrm{Gal}(\mathbb{K}/\mathbb{L})| \\ &\le |\mathrm{Gal}(\mathbb{L}/\Bbbk)| \le [\mathbb{L} : \Bbbk],\end{aligned}$$

with equality at the first $\le$ sign only if $\varphi \mapsto \overline{\varphi}$ is onto $\mathrm{Gal}(\mathbb{L}/\Bbbk)$ and with equality at the second $\le$ sign only if $\mathbb{L}$ is the splitting field over $\Bbbk$ of the minimal polynomial of a certain element γ of $\mathbb{L}$. Equality must hold in both cases because the end members of the display are equal, and we conclude that $\varphi \mapsto \overline{\varphi}$ is onto and that $\mathbb{L}/\Bbbk$ is a normal extension.

We are left with proving that if $\mathbb{L}/\Bbbk$ is a normal extension, then H is a normal subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. Thus let $\mathbb{L}/\Bbbk$ be normal. In view of the conclusion of the first paragraph of the proof, it is enough to prove that $\varphi(\mathbb{L}) = \mathbb{L}$ for all $\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk)$. By definition of normal extension, $\mathbb{L}$ is the splitting field of some polynomial $F(X)$ in $\Bbbk[X]$. We may assume that $F(X)$ is monic. Let us write

$$F(X) = (X - x_1) \cdots (X - x_n) \qquad \text{with all } x_j \text{ in } \mathbb{L}.$$

Applying a given member φ of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ to the coefficients, we obtain

$$F(X) = (X - \varphi(x_1)) \cdots (X - \varphi(x_n)),$$

and here the $\varphi(x_j)$'s are known only to be in $\mathbb{K}$. By unique factorization in $\mathbb{K}[X]$, $\varphi(x_i) = x_{j(i)}$ for some $j = j(i)$. Therefore $\varphi(x_i)$ is in $\mathbb{L}$ for all i. Since $\mathbb{L}$ is the splitting field of $F(X)$ over $\Bbbk$, $\mathbb{L} = \Bbbk(x_1, \ldots, x_n)$. Thus φ maps $\mathbb{L}$ into $\mathbb{L}$. □

The examples of Galois groups given in Section 6 all involved fields that are finite extensions of the rationals $\mathbb{Q}$. As we shall see in Section 17, it is important for the understanding of Galois groups of finite extensions of $\mathbb{Q}$ to be able to identify Galois groups of finite extensions of *finite* fields. This matter is addressed in the following proposition.

Proposition 9.40. Let $\mathbb{K}$ be a finite extension of the finite field $\mathbb{F}_q$, where $q = p^a$ and p is prime, and suppose that $[\mathbb{K} : \mathbb{F}_q] = n$. Then $\mathbb{K}$ is a Galois extension of $\mathbb{F}_q$, the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_q)$ is cyclic of order n, and a generator is the a^{th}-power Frobenius automorphism $x \mapsto x^q = x^{p^a}$.

PROOF. Theorem 9.14 shows that $\mathbb{K}$ is a splitting field for $X^{q^n} - X$ over $\mathbb{F}_p$. Hence it is a splitting field for $X^{q^n} - X$ over $\mathbb{F}_q$, and $\mathbb{K}/\mathbb{F}_q$ is a normal extension. The polynomial $X^{q^n} - X$ has no multiple roots, and it follows that $\mathbb{K}/\mathbb{F}_q$ is a separable extension.

Define φ by $\varphi(x) = x^q$. Lemma 9.18 shows that φ is an automorphism of $\mathbb{K}$. Since every member of $\mathbb{F}_q^\times$ has order dividing $q - 1$, every nonzero element of $\mathbb{F}_q$ is fixed by φ. The map φ certainly carries 0 to 0, and thus φ is in $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_q)$. By a similar argument, φ^n fixes every element of $\mathbb{K}$, and hence $\varphi^n = 1$. Corollary 4.27 shows that $\mathbb{K}^\times$ is cyclic, hence that there exists an element y in $\mathbb{K}^\times$ such that $y^l \neq 1$ for $1 \leq l < q^n - 1$. This y has $y^l \neq y$ for $2 \leq l \leq q^n - 1$. Then $\varphi^k(y) = y^{q^k}$ cannot be 1 for $1 \leq k \leq n - 1$, and φ must have order exactly n. This shows that φ generates a cyclic subgroup of order n in $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_q)$. Since n is an upper bound for the order of $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_q)$ by Proposition 9.33, this cyclic subgroup exhausts the Galois group. □

EXAMPLE. Suppose that we are given a polynomial with coefficients in $\mathbb{F}_p$ and we want to find the Galois group of a splitting field. Since there are efficient computer programs for factoring the polynomial into irreducible polynomials, let us take that factorization as done. The Galois group will be cyclic of some order with generator the Frobenius automorphism $x \mapsto x^p$. For an irreducible polynomial of degree n, a splitting field has degree n, and the smallest power of $x \mapsto x^p$ that gives the identity is the n^{th} power. The conclusion is that the Galois group is cyclic of order equal to the least common multiple of the degrees of the irreducible constituents, a generator being the Frobenius automorphism.

Pure Mathematical Physics

9. Application to Constructibility of Regular Polygons

In this section we use Galois theory to give a proof of Theorem 9.25 concerning the constructibility of regular n-gons. Let us recall the statement.

THEOREM 9.25 (Gauss). A regular n-gon is constructible with straightedge and compass if and only if n is the product of distinct Fermat primes and a power of 2.

PROOF OF SUFFICIENCY. First suppose that n is a Fermat prime $n = 2^{2^N} + 1$. Let $\mathbb{K} = \mathbb{Q}(e^{2\pi i/n})$. We saw in Section 5 that the degree $[\mathbb{K} : \mathbb{Q}]$ is 2^{2^N}, hence is a power of 2. Furthermore we know that $\mathbb{K}$ is a separable extension of $\mathbb{Q}$, being of characteristic 0, and it is normal, being the splitting field for $X^n - 1$ over $\mathbb{Q}$. In Section 6 we saw that the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is cyclic of order 2^{2^N}. Let c be a generator of this group. For each integer k with $0 \le k \le 2^N$, let H_{2^k} be the unique cyclic subgroup of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ of order 2^k. For this subgroup, $c^{2^{2^N-k}}$ is a generator. Put $\mathbb{L}_{2^k} = \mathbb{K}^{H_{2^k}}$. Then we have inclusions

$$\{1\} \subseteq H_2 \subseteq H_{2^2} \subseteq \cdots H_{2^k} \subseteq \cdots \subseteq H_{2^{2^N-1}} \subseteq H_{2^{2^N}} = \mathrm{Gal}(\mathbb{K}/\mathbb{Q}),$$

the index being 2 at each stage. Theorem 9.38 says that the correspondence with intermediate fields reverses inclusions and that the degree of each consecutive extension of subfields matches the index of the corresponding consecutive subgroups. The intermediate fields are therefore of the form

$$\mathbb{K} \supseteq \mathbb{L}_2 \supseteq \mathbb{L}_{2^2} \supseteq \cdots \mathbb{L}_{2^k} \supseteq \cdots \supseteq \mathbb{L}_{2^{2^N-1}} \supseteq \mathbb{L}_{2^{2^N}} = \mathbb{Q},$$

and the degree in each case is 2. In view of the formula for the roots of a quadratic polynomial, each extension is obtained by adjoining some square root. By Theorem 9.24 the members of $\mathbb{K}$ are constructible with straightedge and compass. In particular, $e^{2\pi i/n}$ is constructible, and a regular n-gon is constructible.

Next suppose that $e^{2\pi i/r}$ and $e^{2\pi i/s}$ are both constructible and that $\mathrm{GCD}(r, s) = 1$. Choose integers a and b with $ar + bs = 1$, so that $\frac{a}{s} + \frac{b}{r} = \frac{1}{rs}$. Then the equality $(e^{2\pi i/s})^a (e^{2\pi i/r})^b = e^{2\pi i/(rs)}$ shows that $e^{2\pi i/(rs)}$ is constructible. This proves the sufficiency for any product of distinct Fermat primes. Bisection of an angle is always possible with straightedge and compass, as was observed in the third paragraph of Section 5, and the proof of the sufficiency in Theorem 9.25 is therefore complete. □

REMARKS. The above proof shows that the construction is possible, but it gives little clue how to carry out the construction. We shall address this matter further in Section 12.

Pure Mathematical Physics

We turn our attention to the necessity—that n has to be the product of distinct Fermat primes and a power of 2 if a regular n-gon is constructible. For the moment let $n \geq 1$ be any integer. Let us consider the distinct n^{th} roots of 1 in $\mathbb{C}$, which are $e^{k2\pi i/n}$ for $0 \leq k < n$. The order of each of these elements divides n, and the order is exactly n if and only if $\text{GCD}(k, n) = 1$. In this case we say that $e^{k2\pi i/n}$ is a **primitive** n^{th} root of 1. Define the **cyclotomic polynomial** $\Phi_n(X)$ by

$$\Phi_n(X) = \prod_{\substack{\text{GCD}(k,n)=1,\\ 0\leq k<n}} (X - e^{k2\pi i/n}).$$

Each such polynomial is monic by inspection. The splitting field $\mathbb{Q}(e^{2\pi i/n})$ in $\mathbb{C}$ is called a **cyclotomic field**. Since the complex roots of $X^n - 1$ are exactly the numbers $e^{k2\pi i/n}$, we have

$$X^n - 1 = \prod_{d|n} \Phi_d(X),$$

the product being taken over the positive divisors d of n.

Lemma 9.41. Each cyclotomic polynomial $\Phi_n(X)$ lies in $\mathbb{Z}[X]$, and the degree of $\Phi_n(X)$ is $\varphi(n)$, where φ is the Euler φ function defined just before Corollary 1.10.

PROOF. We know that $\Phi_n(X)$ is in $\mathbb{C}[X]$, and we begin by showing by induction on n that $\Phi_n(X)$ is in $\mathbb{Q}[X]$. For $n = 1$, we have $\Phi_1[X] = X - 1$, and the assertion is true. If it is true for all d with $1 \leq d < n$, then the formula $X^n - 1 = \prod_{d|n} \Phi_d(X)$ and induction show that $X^n - 1 = \Phi_n(X)F(X)$ for some $F(X)$ in $\mathbb{Q}[X]$. By the division algorithm, $X^n - 1 = F(X)Q(X) + R(X)$ for polynomials $Q(X)$ and $R(X)$ in $\mathbb{Q}[X]$ with $R(X) = 0$ or $\deg R(X) < \deg F(X)$. Subtraction gives $F(X)\big(\Phi_n(X) - Q(X)\big) = -R(X)$ in $\mathbb{C}[X]$. If $R(X)$ is not 0, then $\deg R(X) < \deg F(X)$ gives a contradiction. Therefore $R(X) = 0$ and $F(X)\big(\Phi_n(X) - Q(X)\big) = 0$. Since $\mathbb{C}[X]$ is an integral domain, $\Phi_n(X) = Q(X)$. Thus $\Phi_n(X)$ is in $\mathbb{Q}[X]$, and the induction is complete.

To see that $\Phi_n(X)$ is in $\mathbb{Z}[X]$, we again induct, the case $n = 1$ being clear. The formula $X^n - 1 = \prod_{d|n} \Phi_d(X)$ and induction show that $X^n - 1 = \Phi_n(X)F(X)$ for some $F(X)$ in $\mathbb{Z}[X]$. Since $\Phi_n(X)$ is known to be in $\mathbb{Q}[X]$, Corollary 8.20c shows that $\Phi_n(X)$ is in $\mathbb{Z}[X]$, and the induction is complete. □

Lemma 9.42. Each cyclotomic polynomial $\Phi_n(X)$ is irreducible as a member of $\mathbb{Q}[X]$.

PROOF. Let ζ be a primitive n^{th} root of 1, let p be a prime number not dividing n, let $F(X)$ be the minimal polynomial of ζ over $\mathbb{Q}$, and let $G(X)$ be the minimal polynomial of ζ^p. The main step is to show that $F(X) = G(X)$.

To carry out this step, we observe that $F(\zeta) = G(\zeta^p) = 0$ and that $F(X)$ and $G(X)$ must divide $\Phi_n(X)$. Arguing by contradiction, suppose that $F(X) \neq G(X)$. Then $\text{GCD}(F, G) = 1$ since $F(X)$ and $G(X)$ are irreducible over $\mathbb{Q}$, and therefore $F(X)G(X)$ divides $\Phi_n(X)$. Hence we can write

$$X^n - 1 = F(X)G(X)H(X),$$

and $H(X)$ is a monic member of $\mathbb{Z}[X]$ by Lemma 9.41 and Corollary 8.20c. Since ζ is a root of $G(X^p)$, we must have $G(X^p) = F(X)M(X)$ for some monic polynomial $M(X)$ in $\mathbb{Z}[X]$. We apply the substitution homomorphism to $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ that carries X to X and reduces the coefficients modulo p; the mapping on the coefficients will be denoted by a bar. Then we have

$$X^n - \bar{1} = \overline{F}(X)\overline{G}(X)\overline{H}(X) \qquad \text{and} \qquad \overline{G}(X)^p = \overline{G}(X^p) = \overline{F}(X)\overline{M}(X),$$

the equality $\overline{G}(X)^p = \overline{G}(X^p)$ following from Lemma 9.18. If $\overline{Q}(X)$ is a prime factor of $\overline{F}(X)$, then $\overline{Q}(X)$ divides $\overline{G}(X)^p$ and therefore must divide $\overline{G}(X)$. So $\overline{Q}(X)^2$ divides $X^n - \bar{1}$. Therefore $X^n - \bar{1}$ has multiple roots in its splitting field, in contradiction to Corollary 9.17 and the fact that the derivative of $X^n - \bar{1}$ is nonzero at each nonzero member of $\mathbb{F}_p$ (since $\text{GCD}(p, n) = 1$ by assumption). We conclude that $F(X) = G(X)$.

Now suppose that r is a positive integer with $\text{GCD}(r, n) = 1$. Then we can write $r = p_1 \cdots p_l$ with each p_j not dividing n, and we see inductively that ζ^r has $F(X)$ as minimal polynomial. Thus $F(X)$ has at least $\varphi(n)$ roots. Since $F(X)$ divides $\Phi_n(X)$, we must have $F(X) = \Phi_n(X)$. Therefore $\Phi_n(X)$ is irreducible over $\mathbb{Q}$. □

PROOF OF NECESSITY IN THEOREM 9.25. Theorem 9.24 shows that the degree $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}]$ must be a power of 2 if a regular n-gon is constructible. Since $e^{2\pi i/n}$ is a root of $\Phi_n(X)$ and since Lemma 9.42 shows $\Phi_n(X)$ to be irreducible over $\mathbb{Q}$, $\Phi_n(X)$ is the minimal polynomial of $e^{2\pi i/n}$ over $\mathbb{Q}$. By Lemma 9.41 the degree in question is given by $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \varphi(n)$, where φ is the Euler φ function. Corollary 1.10 shows that if $n = p_1^{k_1} \cdots p_r^{k_r}$ is a prime factorization of n into distinct prime powers with each $k_j > 0$, then

$$\varphi(n) = \prod_{j=1}^{r} p_j^{k_j - 1}(p_j - 1).$$

For constructibility this must be a power of 2. Then each p_j dividing n must be 1 more than a power of 2, i.e., must be 2 or a Fermat prime, and the only p_j allowed to have p_j^2 dividing n is $p_j = 2$.

10. Application to Proving the Fundamental Theorem of Algebra

In this section we use Galois theory to give a proof of the Fundamental Theorem of Algebra. Let us recall the statement.

THEOREM 1.18 (Fundamental Theorem of Algebra). Any polynomial in $\mathbb{C}[X]$ with degree ≥ 1 has at least one root.

We begin with a lemma that handles three easy special cases.

Lemma 9.43. There are no finite extensions of $\mathbb{R}$ of odd degree greater than 1, the only extension of $\mathbb{R}$ of degree 2 up to $\mathbb{R}$ isomorphism is $\mathbb{C}$, and there are no finite extensions of $\mathbb{C}$ of degree 2.

PROOF. If $\mathbb{K}$ is a finite extension of $\mathbb{R}$ of odd degree and if x is in $\mathbb{K}$, then $[\mathbb{R}(x) : \mathbb{R}]$ is odd, and consequently the minimal polynomial $F(X)$ of x over $\mathbb{R}$ is irreducible of odd degree. By Proposition 1.20, which is derived from the Intermediate Value Theorem of Section A3 of the appendix, $F(X)$ has at least one root in $\mathbb{R}$. Therefore $F(X)$ has degree 1, and x is in $\mathbb{R}$.

If $F(X)$ is an irreducible polynomial in $\mathbb{R}[X]$ of degree 2, then $F(X)$ splits in $\mathbb{C}$ by the quadratic formula, and hence the only extension of $\mathbb{R}$ of degree 2 is $\mathbb{C}$, up to $\mathbb{R}$ isomorphism, by the uniqueness of splitting fields (Theorem 9.13).

Let $G(X) = X^2 + bX + c$ be a polynomial in $\mathbb{C}[X]$ of degree 2. Then $G(X)$ has a root x in $\mathbb{C}$ given by the quadratic formula since every member of $\mathbb{C}$ has a square root[8] in $\mathbb{C}$, and $G(X)$ cannot be irreducible. Since any finite extension of $\mathbb{C}$ of degree 2 would have to be of the form $\mathbb{C}(x)$, with x equal to a root of an irreducible quadratic polynomial over $\mathbb{C}$, there can be no such extension. □

PROOF OF THEOREM 1.18. First let us show that every irreducible member $F(X)$ of $\mathbb{R}[X]$ splits over $\mathbb{C}$. Let $\mathbb{K}$ be a splitting field for $F(X)$. Say that $[\mathbb{K} : \mathbb{R}] = 2^m N$ with N odd. Then $\mathbb{K}$ is a Galois extension of $\mathbb{R}$, and $|\operatorname{Gal}(\mathbb{K}/\mathbb{R})| = 2^m N$. By the Sylow Theorems (particularly Theorem 4.59a), let H be a Sylow 2-subgroup of $\operatorname{Gal}(\mathbb{K}/\mathbb{R})$. This H has $|H| = 2^m$. The field $\mathbb{L} = \mathbb{K}^H$ that corresponds to H under Theorem 9.38 has $[\mathbb{L} : \mathbb{R}] = N$ with N odd, and the first conclusion of Lemma 9.43 shows that $N = 1$. Thus $|\operatorname{Gal}(\mathbb{K}/\mathbb{R})| = 2^m$. Corollary 4.40 shows that $\operatorname{Gal}(\mathbb{K}/\mathbb{R})$ has nested subgroups of all orders 2^{m-k} with $0 \leq k \leq m$, and Theorem 9.38 says that the corresponding fixed fields are nested and have respective degrees 2^k with $0 \leq k \leq m$. The extension field of $\mathbb{R}$ for $k = 1$ is necessarily $\mathbb{C}$ by Lemma 9.43, and Lemma 9.43 shows that there

[8] To see that every member of $\mathbb{C}$ has a square root in $\mathbb{C}$, let $c + di$ be given with c and d real and with $d \neq 0$. Let a and b be real numbers with $a^2 = \frac{1}{2}(c + \sqrt{c^2 + d^2})$, $b^2 = \frac{1}{2}(-c + \sqrt{c^2 + d^2})$, and $\operatorname{sgn}(ab) = \operatorname{sgn} d$. Then $(a + bi)^2 = c + di$.

Pure Mathematical Physics

are no quadratic extensions of $\mathbb{C}$. Therefore $m = 0$ or $m = 1$, and the possible splitting fields for $F(X)$ are $\mathbb{R}$ and $\mathbb{C}$ in the two cases.

To complete the proof, suppose that $\mathbb{K}$ is a finite algebraic extension of $\mathbb{C}$ of degree n. Then $\mathbb{K}$ is a finite algebraic extension of $\mathbb{R}$ of degree $2n$. The Theorem of the Primitive Element allows us to write $\mathbb{K} = \mathbb{R}(x)$ for some $x \in \mathbb{K}$, and the minimal polynomial of x over $\mathbb{R}$ necessarily has degree $2n$. The previous paragraph shows that this polynomial splits in $\mathbb{C}$. Thus x is in $\mathbb{C}$, and $\mathbb{K} = \mathbb{C}$. This completes the proof. □

11. Application to Unsolvability of Polynomial Equations with Nonsolvable Galois Group

The quadratic formula for finding the roots of a quadratic polynomial has in principle been known since the time of the Babylonians about 400 B.C.[9] The corresponding problem of finding roots of cubics was unsolved until the sixteenth century, and **Cardan's formula** was discovered at that time. The original formula assumes real coefficients and was in two parts, a first case corresponding to what we now view as one real root and two complex roots, the second case corresponding to what we view as three real roots.[10] There is a similar formula, but more complicated, for solving quartics. Further centuries passed with no progress on finding a corresponding formula for the roots of a polynomial of degree 5 or higher. The introduction of Galois theory in the early nineteenth century made it possible to prove a surprising negative statement about all degrees beyond 4.

Suppose that we are given a polynomial equation with coefficients in the field $\mathbb{Q}$ or a more general field $\Bbbk$ of characteristic 0. In this section we use Galois theory to address the question whether the roots of the equation in a splitting field can be expressed in terms of $\Bbbk$ and the adjunction of finitely many n^{th} roots to the field, for various values of n. For the moment let us say in this case that the roots are "expressible in terms of the members of $\Bbbk$ and radicals." We shall make this notion more precise shortly.

Recall from Section IV.8 that with a finite group G, we can find a strictly decreasing sequence of subgroups starting with G and ending with $\{1\}$ such

[9]The Babylonians did not actually have equations but had an algorithmic method that amounted to completing the square.

[10]Cardan's name was Girolamo Cardano. The solution in the first case of the cubic seems to have been discovered by Scipione dal Ferro and later by Nicolo Tartaglia. Dal Ferro died in 1526 and passed the secret method to his student Antonio Fior. In 1535 Fior engaged in a public contest with Tartaglia at solving cubics, and he lost. Cardano wheedled the solution method in the first case from Tartaglia, published it in 1539, and discovered and published the solution in the second case. Cardano's student Lodovico Ferrari discovered how to solve quartics, and Cardano published that solution as well. See "St. Andrews" in the Selected References for more information.

that each subgroup is normal in the next larger one and each quotient group is simple. Such a series was defined to be a composition series for G. The Jordan–Hölder Theorem (Corollary 4.50) says that the respective consecutive quotients are isomorphic for any two composition series, apart from the order in which they appear. We define the finite group G to be **solvable** if each of the consecutive quotients is cyclic of prime order, rather than nonabelian. It is enough that the group have a normal series for which each of the consecutive quotients is abelian.

Examples of solvable and nonsolvable groups are obtainable from the calculations in Section IV.8: abelian groups and groups of prime-power order are always solvable, the symmetric group $\mathfrak{S}_4$ and each of its subgroups are solvable, and the symmetric group $\mathfrak{S}_5$ is not solvable since a composition series is $\mathfrak{S}_5 \supseteq \mathfrak{A}_5 \supseteq \{1\}$ and the group $\mathfrak{A}_5$ is simple (Theorem 4.47).

Modulo a precise definition for a field $\Bbbk$ of the words "expressible in terms of the members of $\Bbbk$ and radicals," the answer to our main question is as follows.

Theorem 9.44 (Abel, Galois).[11] Let $\Bbbk$ be a field of characteristic 0, let $F(X)$ be in $\Bbbk[X]$, and let $\mathbb{K}$ be a splitting field of $F(X)$ over $\Bbbk$. Then the roots of $F(X)$ are expressible in terms of the members of $\Bbbk$ and radicals if and only if the group $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is solvable.

EXAMPLE. With $\Bbbk = \mathbb{Q}$, let $F(X)$ be the polynomial $F(X) = X^5 - 5X + 1$ in $\mathbb{Q}[X]$. We shall show that

(i) $F(X)$ is irreducible over $\mathbb{Q}$,
(ii) $F(X)$ has three roots in $\mathbb{R}$ and one pair of conjugate complex roots in $\mathbb{C}$,
(iii) the splitting field $\mathbb{K}$ over $\mathbb{Q}$ of any polynomial of degree 5 for which (i) and (ii) hold has Galois group with $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathfrak{S}_5$.

We know that from Theorem 4.47 that $\mathfrak{S}_5$ is not solvable, and Theorem 9.44 therefore allows us to conclude that the roots of $X^5 - 5X + 1$ are not expressible in terms of the members of $\mathbb{Q}$ and radicals.

To prove (i), we apply Eisenstein's criterion (Corollary 8.22) to the polynomial $F(X-1) = X^5 - 5X^4 + 10X^3 - 10X^2 + 5$ and to the prime $p = 5$, and the irreducibility is immediate.

To prove (ii), we observe that $F(-2) < 0$, $F(0) > 0$, $F(1) < 0$, $F(2) > 0$. Applying the Intermediate Value Theorem (Section A3 of the appendix), we see that there are at least three roots in $\mathbb{R}$. Since $F'(X) = 5(X^4 - 1)$ has exactly the two roots ± 1 in $\mathbb{R}$, $F(X)$ has at most three roots in $\mathbb{R}$ by an application of the Mean Value Theorem.

To prove (iii), label the roots 1, 2, 3, 4, 5 with 1 and 2 denoting the nonreal roots. Each member of the Galois group permutes the roots and is determined

[11] Abel proved that there is no general solution via radicals that gives the roots of polynomials of degree 5. Galois found the present theorem, which shows how to decide the question for each individual polynomial of degree 5.

Pure Mathematical Physics

by its effect on the roots. Thus $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ may be regarded as a subgroup of $\mathfrak{S}_5$. Since $F(X)$ is irreducible over $\mathbb{Q}$, 5 divides $[\mathbb{K} : \mathbb{Q}]$ and 5 divides $|\mathrm{Gal}(\mathbb{K}/\mathbb{Q})|$. By the Sylow Theorems, $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ contains an element of order 5, hence a 5-cycle. Some power of this 5-cycle carries root 1 to root 2. So we may assume that the 5-cycle is (1 2 3 4 5). Also, $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ contains complex conjugation, which acts as (1 2). Then $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ contains

$$\begin{aligned}
&(1\ 2\ 3\ 4\ 5)(1\ 2)(1\ 2\ 3\ 4\ 5)^{-1} = (2\ 3),\\
&(1\ 2\ 3\ 4\ 5)(2\ 3)(1\ 2\ 3\ 4\ 5)^{-1} = (3\ 4),\\
&(1\ 2\ 3\ 4\ 5)(3\ 4)(1\ 2\ 3\ 4\ 5)^{-1} = (4\ 5).
\end{aligned}$$

Since the set $\{(1\ 2),\ (2\ 3),\ (3\ 4),\ (4\ 5)\}$ of transpositions is easily shown from Corollary 1.22 to generate $\mathfrak{S}_5$, $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \mathfrak{S}_5$.

Let $\mathbb{K}'$ be a finite extension of the given field $\Bbbk$. A **root tower** for $\mathbb{K}'$ over $\Bbbk$ is a finite sequence of extensions

$$\Bbbk = \mathbb{K}'_0 \subseteq \mathbb{K}'_1 \subseteq \cdots \subseteq \mathbb{K}'_{l-1} \subseteq \mathbb{K}'_l = \mathbb{K}'$$

such that for each i with $0 \le i \le l-1$, there is a prime number $n_i > 1$ and there is an element r_i in $\mathbb{K}'_{i+1}$ with $a_i = r_i^{n_i}$ in $\mathbb{K}'_i$ and r_i not in $\mathbb{K}'_i$. Then it follows that r_i^k is not in $\mathbb{K}'_i$ for any k with $0 < k < n_i$.

(If we write $a_i = r_i^{n_i}$, then we might think of writing $\mathbb{K}'_{i+1} = \mathbb{K}'_i(\sqrt[n_i]{a_i})$, but this formulation is less precise at the moment since it does not specify precisely which choice of $\sqrt[n_i]{a_i}$ is to be used.)

With "root tower" now well defined, we can make a precise definition and thereby complete the precise formulation of Theorem 9.44. Let $\Bbbk$ be the given field of characteristic 0, let $F(X)$ be in $\Bbbk[X]$, and let $\mathbb{K}$ be a splitting field of $F(X)$ over $\Bbbk$. We say that the roots of $F(X)$ are **expressible in terms of members of $\Bbbk$ and radicals** if there exists some finite extension $\mathbb{K}'$ of $\mathbb{K}$ having a root tower over $\Bbbk$.

The statement of Theorem 9.44 is now completely precise, and the remainder of the section will be devoted to the proof of one direction of the theorem: if the roots are expressible in terms of members of $\Bbbk$ and radicals, then the Galois group is solvable. The proof of the converse direction of the theorem is postponed to Section 13. We begin with a lemma.

Lemma 9.45. Let $\Bbbk$ be a field of any characteristic, and let p be a prime number. If a is a member of $\Bbbk$ such that $X^p - a$ has no root in $\Bbbk$, then $X^p - a$ is irreducible in $\Bbbk$.

Pure Mathematical Physics

PROOF. First suppose that p is different from the characteristic. Let $\mathbb{L}$ be a splitting field for $X^p - a$. The derivative of $X^p - a$, evaluated at any root of $X^p - a$ in $\mathbb{L}$, is nonzero, and Corollary 9.17 shows that $X^p - a$ splits as the product of p distinct linear factors in $\mathbb{L}$. The quotient of any two roots of $X^p - a$ is a p^{th} root of 1. Fixing one of these two roots of $X^p - a$ and letting the other vary, we obtain p distinct p^{th} roots of 1. Thus $\mathbb{L}$ contains all p of the p^{th} roots of 1. Proposition 4.26 shows that the group of p^{th} roots of 1 is cyclic. Let ζ be a generator. If $a^{1/p}$ denotes one of the roots of $X^p - a$ in $\mathbb{L}$, then the set of all the roots is given by $\{a^{1/p}\zeta^k \mid 0 \le k \le p-1\}$.

Now suppose that $X^p - a$ has a nontrivial factorization $X^p - a = F(X)G(X)$ in $\Bbbk[X]$. Possibly by adjusting the leading coefficients of $F(X)$ and $G(X)$, we may assume that $F(X)$ and $G(X)$ are both monic. Unique factorization in $\mathbb{L}[X]$ then implies that there is a nonempty subset S of $\{k \mid 0 \le k \le p-1\}$ with a nonempty complement S^c such that

$$F(X) = \prod_{k\in S} (X - \zeta^k a^{1/p}) \qquad \text{and} \qquad G(X) = \prod_{k\in S^c} (X - \zeta^k a^{1/p}).$$

If S has m elements, then the constant term of $F(X)$ is $(-a^{1/p})^m\omega$, where ω is some p^{th} root of 1. Thus $x = (a^{1/p})^m\omega$ is in $\Bbbk$. Since $\text{GCD}(m, p) = 1$, we can choose integers c and d with $cm + dp = 1$. Since x is in $\Bbbk$, so is $x^c a^d = (a^{1/p})^{mc+dp}\omega^c = a^{1/p}\omega^c$. But $a^{1/p}\omega^c$ is a root of $X^p - a$, in contradiction to the hypothesis that no root of $X^p - a$ lies in $\Bbbk$. Hence $X^p - a$ is irreducible.

If p equals the characteristic of $\Bbbk$, then Lemma 9.18 gives the factorization $X^p - a = (X - a^{1/p})^p$, where $a^{1/p}$ is one root of $X^p - a$ in $\mathbb{K}$. Then we can argue as above except that ζ and ω are to be replaced by 1 throughout. This completes the proof of the lemma. □

PROOF OF NECESSITY IN THEOREM 9.44 THAT $\text{Gal}(\mathbb{K}/\Bbbk)$ BE SOLVABLE. We are to prove that if some finite extension $\mathbb{K}'$ of $\mathbb{K}$ has a root tower over $\Bbbk$, then $\text{Gal}(\mathbb{K}/\Bbbk)$ is solvable.

Step 1. We enlarge each field in the given root tower to obtain a root tower

$$\Bbbk \subseteq \mathbb{K}_0'' \subseteq \mathbb{K}_1'' \subseteq \cdots \subseteq \mathbb{K}_{l-1}'' \subseteq \mathbb{K}_l'' = \mathbb{K}''$$

of a finite extension $\mathbb{K}''$ of $\mathbb{K}'$ in such a way that $\mathbb{K}_0''$ is the normal extension of $\Bbbk$ obtained by adjoining all n^{th} roots of 1 for a suitably large n and such that each $\mathbb{K}_{i+1}''$ is the normal extension of $\mathbb{K}_i''$ for $0 \le i \le l-1$ obtained by adjoining all n_i^{th} roots of the member a_i of $\mathbb{K}_i'$. Using Theorem 9.22, choose an algebraic closure $\overline{\mathbb{K}'}$ of $\mathbb{K}'$. Let n be the product of the integers $n_0, n_1, \ldots, n_{l-1}$. Let $\zeta_1, \ldots, \zeta_{n-1}$ be the n^{th} roots of 1 in $\overline{\mathbb{K}'}$ other than 1 itself, define subfields of $\overline{\mathbb{K}'}$ by

$$\mathbb{K}_i'' = \mathbb{K}_i'(\zeta_1, \ldots, \zeta_{n-1}) \qquad \text{for } 0 \le i \le l,$$

Pure Mathematical Physics

and put $\mathbb{K}'' = \mathbb{K}'_l$. The field $\mathbb{K}''_0$ is a splitting field for $X^n - 1$ over $\Bbbk$ and is therefore a normal extension. The field $\mathbb{K}''_{i+1}$ is given by $\mathbb{K}''_{i+1} = \mathbb{K}''_i(r_i)$, where r_i is a root in $\mathbb{K}''_{i+1}$ of the polynomial $X^{n_i} - a_i$ in $\mathbb{K}''_i[X]$. Here n_i is prime. Lemma 9.45 shows that either r_i is in $\mathbb{K}''_i[X]$ or $X^{n_i} - a_i$ is irreducible in $\mathbb{K}''_i[X]$. In the first case, $\mathbb{K}''_{i+1} = \mathbb{K}''_i$, and we have a normal extension. In the second case, $\mathbb{K}''_{i+1}$ is a splitting field for $X^{n_i} - a_i$ over $\mathbb{K}''_i$ because it is generated by $\mathbb{K}''_i$ and one root of $X^{n_i} - a_i$ and because all n_i^{th} roots of 1 already lie in $\mathbb{K}''_0$; thus again we have a normal extension.

Step 2. The Galois group of $\mathbb{K}''_0$ over $\Bbbk$ is abelian. In fact, Proposition 4.26 shows that the group of n^{th} roots of 1 in $\mathbb{K}''_0$ is cyclic. Let ζ be a generator, and let $U = \{\zeta^k\}_{k=0}^{n-1}$. The map of $\mathrm{Gal}(\mathbb{K}''_0/\Bbbk)$ into $\mathrm{Aut}\, U$ given by $\varphi \mapsto \varphi\big|_U$ is a one-one homomorphism, and $\mathrm{Aut}\, U$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. Since $(\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, it follows that $\mathrm{Gal}(\mathbb{K}''_0/\Bbbk)$ is abelian.

Step 3. The Galois group of $\mathbb{K}''_{i+1}$ over $\mathbb{K}''_i$ is trivial or is cyclic of order n_i. In fact, the Galois group is trivial if $\mathbb{K}''_{i+1} = \mathbb{K}''_i$. The contrary case is that $[\mathbb{K}''_{i+1} : \mathbb{K}''_i] = n_i$, and then $\mathrm{Gal}(\mathbb{K}''_{i+1}/\mathbb{K}''_i)$ has order n_i, which is prime. Every group of order n_i is cyclic, and hence $\mathrm{Gal}(\mathbb{K}''_{i+1}/\mathbb{K}''_i)$ is cyclic.

Step 4. We extend the root tower to a larger field $\mathbb{L} \supseteq \mathbb{K}''$ that is a normal extension of $\Bbbk$. The resulting root tower of $\mathbb{L}$ will be written as

$$\begin{aligned}\Bbbk \subseteq \mathbb{L}_0 = \mathbb{K}''_0 \subseteq \mathbb{L}_1 = \mathbb{K}''_1 \subseteq \cdots \\ \subseteq \mathbb{L}_{k-1} = \mathbb{K}''_{l-1} \subseteq \mathbb{L}_l = \mathbb{K}'' \subseteq \mathbb{L}_{l+1} \subseteq \cdots \subseteq \mathbb{L}_t = \mathbb{L}.\end{aligned}$$

As it is, we cannot say that $\mathbb{K}''$ is the splitting field over $\Bbbk$ for the product of the minimal polynomials used in Step 1, because the elements a_i are not assumed to lie in $\Bbbk$. To adjust the tower to correct this problem, write $\mathbb{K}''$ as

$$\mathbb{K}'' = \Bbbk(r_0, r_1, \ldots, r_{l-1}, \zeta) = \Bbbk(x_0, \ldots, x_l),$$

with ζ as in Step 2. Here $r_0, \ldots, r_{l-1}$ are the given elements that define the original root tower, and we define $x_l = \zeta$ and $x_j = r_j$ for $0 \le j < l$. Since $\mathbb{K}''$ is a finite extension of $\Bbbk$, each x_j has a minimal polynomial $G_j(X)$ over $\Bbbk$. Define $G(X) = \prod_{j=0}^{l} G_j(X)$, and let $\mathbb{L}$ be the splitting field of $G(X)$ in the algebraic closure $\overline{\mathbb{K}'}$. The field $\mathbb{L}$ is a normal extension of $\Bbbk$. The roots of $G(X)$ are the members of $\mathbb{L}$ that are roots of some $G_j(X)$. Each x_j is a root of its own $G_j(X)$. If x'_j is another root of $G_j(X)$, then there is a $\Bbbk$ isomorphism of $\Bbbk(x_j)$ onto $\Bbbk(x'_j)$, and we know by the uniqueness of splitting fields (Theorem 9.13′)[12] that this

[12]The theorem is to be applied to $\sigma : \Bbbk(x_j) \to \Bbbk(x'_j)$ with $F(X) = F^\sigma(X) = G(X)$ and with $\mathbb{L}' = \mathbb{L}$.

Pure Mathematical Physics

extends to a $\Bbbk$ isomorphism of $\mathbb{L}$ onto $\mathbb{L}$. Hence to each root θ of $G(X)$ in $\mathbb{L}$ corresponds some x_j and some $\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk)$ with $\varphi(x_j) = \theta$. Thus

$$\mathbb{L} = \Bbbk\big(\{\varphi(x_j) \mid 0 \le j \le l \text{ and } \varphi \in \mathrm{Gal}(\mathbb{L}/\Bbbk\}\big).$$

For any φ in $\mathrm{Gal}(\mathbb{L}/\Bbbk)$ and any $j \le l-1$, the element $\varphi(x_j)$ of $\mathbb{L}$ satisfies

$$(\varphi(x_j))^{n_j} = \varphi(x_j^{n_j}) = \varphi(a_j),$$

and the element on the right is in $\varphi(K_j'')$. Any element $\varphi(\zeta)$ is an n^{th} root of 1 and hence is already in $\mathbb{K}_0''$; such elements are redundant for $\varphi \neq 1$. Enumerate $\mathrm{Gal}(\mathbb{L}/\Bbbk)$ as $\varphi_1, \dots, \varphi_s$ with $\varphi_1 = 1$. The tower for $\mathbb{K}''$ is to be continued with the fields obtained by adjoining one at a time the elements

$$\varphi_2(r_0), \dots, \varphi_2(r_{l-1}), \varphi_3(r_0), \dots, \varphi_3(r_{l-1}), \quad \dots, \quad \varphi_s(r_0), \dots, \varphi_s(r_{l-1}).$$

The final field is $\mathbb{L}$, and then we have an enlarged tower as asserted.

Step 5. $\mathrm{Gal}(\mathbb{L}/\Bbbk)$ is a solvable group. In fact, first we prove by induction downward on i that $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_i)$ is solvable, the case $i = t$ being the case of the trivial group. Let $i < t$ be given. We have arranged that $\mathbb{L}_{i+1}$ is a normal extension of $\mathbb{L}_i$. Since $\mathbb{L}$ is normal over all the smaller fields by Step 4, Corollary 9.39 therefore gives $\mathrm{Gal}(\mathbb{L}_{i+1}/\mathbb{L}_i) \cong \mathrm{Gal}(\mathbb{L}/\mathbb{L}_i) \big/ \mathrm{Gal}(\mathbb{L}/\mathbb{L}_{i+1})$. The group on the left side is cyclic by Step 3 or the analogous proof with some r_j replaced by a suitable $\varphi(r_j)$, and thus a normal series with abelian quotients for $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_{i+1})$ may be extended by including the term $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_i)$, and the result is still a normal series with abelian quotients. Thus $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_i)$ is solvable. This completes the induction and shows that $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_0)$ is solvable. To complete the proof we use the isomorphism $\mathrm{Gal}(\mathbb{L}_0/\Bbbk) \cong \mathrm{Gal}(\mathbb{L}/\Bbbk) \big/ \mathrm{Gal}(\mathbb{L}/\mathbb{L}_0)$ given by Corollary 9.39. The group on the left side is abelian by Step 2, and thus a normal series with abelian quotients for $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_0)$ may be extended by including the term $\mathrm{Gal}(\mathbb{L}/\Bbbk)$, and the result is still a normal series with abelian quotients. Thus $\mathrm{Gal}(\mathbb{L}/\Bbbk)$ is solvable.

Step 6. $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is a solvable group. We have $\mathbb{L} \supseteq \mathbb{K} \supseteq \Bbbk$ with $\mathbb{L}/\Bbbk$ normal by Step 4 and with $\mathbb{K}/\Bbbk$ normal since $\mathbb{K}$ is a splitting field of $F(X)$ over $\Bbbk$. Applying Corollary 9.39, we obtain an isomorphism $\mathrm{Gal}(\mathbb{K}/\Bbbk) \cong \mathrm{Gal}(\mathbb{L}/\Bbbk) \big/ \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Then Step 6 will follow from Step 5 if it is shown that any homomorphic image of a solvable group is solvable. Thus let G be a solvable group, and let $\varphi : G \to H$ be an onto homomorphism. Write $G = G_1 \supseteq \cdots \supseteq G_m = \{1\}$ with abelian quotients, and define $H_i = \varphi(G_i)$. Passage to the quotient gives us a homomorphism φ_i carrying G_i onto H_i/H_{i+1}. Since $\varphi(G_{i+1}) \subseteq H_{i+1}$, φ induces a homomorphism $\overline{\varphi}_i$ of G_i/G_{i+1} onto H_i/H_{i+1}. As the image of an abelian group under a homomorphism, H_i/H_{i+1} is abelian. Therefore H is solvable. This completes the proof. □

Pure Mathematical Physics

12. Construction of Regular Polygons

Theorem 9.25 proved the constructibility of regular n-gons when n is the product of a power of 2 and distinct Fermat primes, but it gave little clue how to carry out the construction. In this section we supply enough further detail so that one can actually carry out the construction. It is enough to handle the case that n is a Fermat prime, $n = 2^{2^N} + 1$, and we shall suppose that n is a prime of this form.

Let $\zeta = e^{2\pi i/n}$. The field of interest is $\mathbb{Q}(\zeta)$, with $[\mathbb{Q}(\zeta) : \mathbb{Q}] = n - 1$. The usual basis of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is $\{1, \zeta, \zeta^2, \ldots, \zeta^{n-2}\}$, but we shall use the basis

$$\{\zeta, \zeta^2, \zeta^3, \ldots, \zeta^{n-1}\}$$

instead, in order to identify the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ more readily with $\mathbb{F}_n^\times$, where $\mathbb{F}_n = \mathbb{Z}/n\mathbb{Z}$ is the field of n elements. In more detail we associate the additive group of $\mathbb{F}_n$ with the additive group of exponents of the members of the cyclic group $\{1, \zeta, \zeta^2, \zeta^3, \ldots, \zeta^{n-1}\}$, and members of the Galois group correspond to the various multiplications of these exponents by $\mathbb{F}_n^\times = \{1, 2, \ldots, n-1\}$. The group $\mathbb{F}_n^\times$ is known to be cyclic of order $n - 1$, and thus the isomorphic Galois group is cyclic. If a generator σ of the Galois group is to correspond to multiplication by a generator g of $\mathbb{F}_n^\times$, then $\sigma(\zeta^s) = \zeta^{gs}$ for all s. With the prime n of the form $2^{2^N} + 1$, let us note for the sake of completeness why we can always take $g = 3$.

Lemma 9.46. The number 3 is a generator of $\mathbb{F}_n^\times$ when n is prime of the form $2^{2^N} + 1$ with $N > 0$.

REMARKS. We verified this assertion for $n = 17$ in Section 6, and in principle one could verify the lemma in any particular case in the same way. Here is a general argument using the law of quadratic reciprocity, whose full statement and proof will be given in Chapter I of *Advanced Algebra*. For a prime number n that is congruent to 1 modulo 4, quadratic reciprocity implies that 3 is a square modulo n if and only if n is a square modulo 3. Since

$$2^{2^N} - 1 = (2^{2^{N-1}} + 1)(2^{2^{N-2}} + 1) \cdots (2^{2^1} + 1)(2^{2^1} - 1)$$

and $2^{2^1} - 1 = 3$, 3 divides $2^{2^N} - 1$. Thus n is congruent to 2 modulo 3, n is not a square modulo 3, and 3 is not a square modulo n. The nonsquares modulo $n = 2^{2^N} + 1$ are exactly the generators of $\mathbb{F}_n^\times$, and therefore 3 is a generator.

Taking Lemma 9.46 into account, we suppose for the remainder of this section that the generator σ of the Galois group corresponds to multiplication of exponents of ζ by 3. Then $\sigma(\zeta) = \zeta^3$ and $\sigma(\zeta^s) = \zeta^{3s}$. These formulas and $\mathbb{Q}$ linearity tell us explicitly how σ operates on all of $\mathbb{Q}(\zeta)$.

Pure Mathematical Physics

The fixed fields that arise within $\mathbb{Q}(\zeta)$ correspond to subgroups of the group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \{\sigma^j \mid 0 \le j < 2^{2^N}\}$, and there is one for each power of 2 from 2^0 to 2^{2^N}. Fix attention on the subgroup H_l of order l, and write $2^{2^N} = kl$, with k and l being powers of 2. A generator of this subgroup is σ^k, and the subgroup is $H_l = \{1, \sigma^k, \sigma^{2k}, \dots, \sigma^{(l-1)k}\}$. Let $\mathbb{K}_l$ be the fixed field of this subgroup, or equivalently of its generator σ^k; this has dimension k over $\mathbb{Q}$.

We shall determine a basis of $\mathbb{K}_l$ over $\mathbb{Q}$. Since $\sigma(\zeta^s) = \zeta^{3s}$, we have $\sigma^k(\zeta^s) = \zeta^{3^k s}$. For $0 \le r \le k-1$, the k elements

$$\eta_r = \zeta^{3^r} + \zeta^{3^{r+k}} + \zeta^{3^{r+2k}} + \cdots + \zeta^{3^{r+k(l-1)}}$$

are linearly independent over $\mathbb{Q}$ because they involve disjoint sets of basis vectors of $\mathbb{Q}(\zeta)$ as r varies. The computation

$$\begin{aligned}
\sigma^k(\eta_r) &= \sigma^k\big(\zeta^{3^r} + \zeta^{3^{r+k}} + \zeta^{3^{r+2k}} + \cdots + \zeta^{3^{r+k(l-1)}}\big) \\
&= \zeta^{3^{r+k}} + \zeta^{3^{r+2k}} + \zeta^{3^{r+3k}} + \cdots + \zeta^{3^{r+kl}} \\
&= \zeta^{3^r} + \zeta^{3^{r+k}} + \zeta^{3^{r+2k}} + \cdots + \zeta^{3^{r+k(l-1)}} \\
&= \eta_r
\end{aligned}$$

shows that each of these vectors is in $\mathbb{K}_l$. Hence $\{\eta_0, \dots, \eta_{k-1}\}$ is a basis of $\mathbb{K}_l$ over $\mathbb{Q}$. The elements of this basis are called the **periods** of l terms of the cyclotomic field.

The extreme cases for the periods are $(k, l) = (2^{2^N}, 1)$, for which $0 \le r \le 2^{2^N} - 1$ with $\eta_r = \zeta^{3^r}$, and $(k, l) = (1, 2^{2^N})$, for which $r = 0$ with

$$\eta_0 = \zeta^{3^0} + \zeta^{3^1} + \zeta^{3^2} + \cdots + \zeta^{3^{2^{2^N}-1}} = \zeta + \zeta^2 + \zeta^3 + \cdots + \zeta^{n-1} = -1.$$

Two facts enter into determining how to write ζ in terms of rationals and square roots. The first is that at stage k for $k \ge 2$, the sum of certain pairs of η_r's is an η for stage $k-1$. The second is that the product of two η_r's at stage k is an integer combination of η's from the same stage and that the sum formulas express this combination in terms of η's from earlier stages. The result is that at the k^{th} stage we obtain expressions for the sum and product of two η_r's in terms of η's from earlier stages. Therefore the two η_r's at stage k are the roots of a quadratic equation whose coefficients involve η's from earlier stages. Consequently we can compute the η_r's explicitly by induction on k. To proceed further, we need to know the formula for the product of two η_r's, which is due to Gauss.

To multiply two η_r's, we need to multiply various powers of ζ, and the exponents get added in the process. This addition is not readily compatible with terms like ζ^{3^r} and ζ^{3^s}, and for that reason Gauss introduced new notation. Define

$$\eta^{(t)} = \zeta^t + \zeta^{t3^k} + \zeta^{t3^{2k}} + \cdots + \zeta^{t3^{k(l-1)}} = \sum_{v \bmod l} \zeta^{t3^{kv}}$$

for $0 \le t \le n-1$. Then $\eta^{(0)} = l$, and for $0 < t \le n-1$, $\eta^{(t)}$ is the η_r in which ζ^t occurs. Gauss's product formula is given by

$$\begin{aligned}
\eta^{(s)}\eta^{(t)} &= \sum_{u \bmod l} \Big(\sum_{v \bmod l} \zeta^{s3^{ku}+t3^{kv}} \Big) \\
&= \sum_{u \bmod l} \Big(\sum_{w \bmod l} \zeta^{s3^{ku}+t3^{k(u+w)}} \Big) \qquad \text{with } v \mapsto u+w \\
&= \sum_{w \bmod l} \Big(\sum_{u \bmod l} \zeta^{(s+t3^{kw})3^{ku}} \Big) \\
&= \sum_{w \bmod l} \eta^{(s+t3^{kw})}.
\end{aligned}$$

In words, this says that to multiply two η's, we add the η's for the exponents obtained by multiplying the first term of $\eta^{(s)}$ by all the terms of $\eta^{(t)}$.

At this point it is more illuminating to work some examples than to try for a general result.

EXAMPLE 1. $n = 5$, $N = 1$, $2^{2^N} = 4$. The relevant pairs (k, l) to study in sequence are $(k, l) = (1, 4), (2, 2), (4, 1)$, and the case $(k, l) = (1, 4)$ is trivial since the only subscripted η is $\sum_{s=0}^{3} \zeta^{3^s} = -1$.

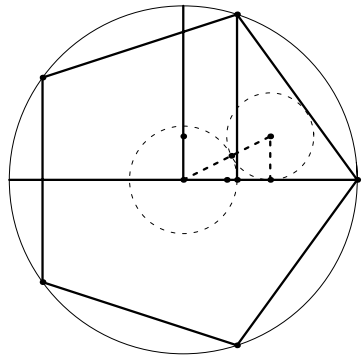


FIGURE 9.3. Construction of a regular pentagon. The circle with center $\left(\frac{1}{2}, \frac{1}{4}\right)$ and radius $\frac{1}{4}$ meets the line from $\left(\frac{1}{2}, \frac{1}{4}\right)$ to the origin at a point at distance $\cos(2\pi/5)$ from the origin.

For $k = 2$, i.e., for the case that there are 2 periods of 2 terms each, we go back to the definition of the η's and find that

$$\begin{aligned}
\eta_0 &= \zeta^{3^{0+2\cdot 0}} + \zeta^{3^{0+2\cdot 1}} = \zeta^1 + \zeta^4, \\
\eta_1 &= \zeta^{3^{1+2\cdot 0}} + \zeta^{3^{1+2\cdot 1}} = \zeta^3 + \zeta^2.
\end{aligned}$$

We form those sums of pairs of η's that yield an η from the previous step. Here there is only one pair, and the sum is given by

$$\eta_0 + \eta_1 = -1.$$

Next we form the elements $\eta^{(t)}$, remembering that for $t > 0$, $\eta^{(t)}$ is the η_r in which ζ^t occurs. Then

$$\eta^{(0)} = 2, \quad \eta^{(1)} = \eta_0, \quad \eta^{(2)} = \eta_1, \quad \eta^{(3)} = \eta_1, \quad \eta^{(4)} = \eta_0.$$

We apply Gauss's product formula to compute the product of the two η's whose sum we have identified. The formula gives

$$\eta_0\eta_1 = \eta^{(1)}\eta^{(2)} = \eta^{(4)} + \eta^{(3)} = \eta_0 + \eta_1 = -1,$$

the second equality following since the rule for the indices is to extract a power of ζ appearing in $\eta^{(1)}$ and add that index to all the powers of ζ appearing in $\eta^{(2)}$. Since η_0 and η_1 have sum -1 and product -1, they are the roots of the quadratic equation

$$x^2 + x - 1 = 0, \qquad \text{namely } \tfrac{1}{2}(-1 \pm \sqrt{5}\,).$$

Deciding which root is η_0 and which is η_1 involves looking at signs. The two roots of the quadratic equation are of opposite sign because the constant term of the quadratic equation is negative. Since $\eta_0 = \zeta + \zeta^{-1} = e^{2\pi i/5} + e^{-2\pi i/5} = 2\cos(2\pi/5)$ is positive, we obtain

$$\eta_0 = \tfrac{1}{2}(-1 + \sqrt{5}\,) \qquad \text{and} \qquad \eta_1 = \tfrac{1}{2}(-1 - \sqrt{5}\,).$$

The computation can in principle stop here, since knowing $\cos(2\pi/5)$ gives us $\sin(2\pi/5)$ and therefore $e^{2\pi i/5}$. See Figure 9.3. But it is instructive to carry out the algorithm anyway. We are thus to treat $k = 4$. The periods of 1 term are

$$\xi_0 = \zeta, \quad \xi_1 = \zeta^3, \quad \xi_2 = \zeta^4, \quad \xi_3 = \zeta^2.$$

The corresponding objects with superscripts are

$$\xi^{(0)} = 1, \quad \xi^{(1)} = \xi_0, \quad \xi^{(2)} = \xi_3, \quad \xi^{(3)} = \xi_1, \quad \xi^{(4)} = \xi_2.$$

The relevant sums of pairs are

$$\xi_0 + \xi_2 = \eta_0,$$
$$\xi_1 + \xi_3 = \xi_1.$$

We again use Gauss's product formula, and this time we obtain

$$\xi_0\xi_2 = \xi^{(1)}\xi^{(4)} = \xi^{(5)} = \xi^{(0)} = 1.$$

Hence ξ_0 and ξ_2 are the roots of the quadratic equation

$$y^2 - \eta_0 y + 1 = 0, \qquad \text{namely } \frac{\frac{-1+\sqrt{5}}{2} \pm i\sqrt{4 - \left(\frac{-1+\sqrt{5}}{2}\right)^2}}{2}.$$

The root y involving the plus sign is $e^{2\pi i/5}$.

EXAMPLE 2.[13] $n = 17,\ N = 2,\ 2^{2^N} = 16$. The relevant pairs (k, l) have $kl = 16$, and the case $(k, l) = (1, 16)$ is trivial since the only subscripted η is $\sum_{s=0}^{15} \zeta^{3^s} = -1$.

For $k = 2$, the 2 periods have 8 terms each, and

$$\begin{aligned}\eta_0 &= \zeta^{3^{0+2\cdot0}} + \zeta^{3^{0+2\cdot1}} + \zeta^{3^{0+2\cdot2}} + \zeta^{3^{0+2\cdot3}} + \zeta^{3^{0+2\cdot4}} + \zeta^{3^{0+2\cdot5}} + \zeta^{3^{0+2\cdot6}} + \zeta^{3^{0+2\cdot7}}\\ &= \zeta^1 + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2,\\ \eta_1 &= \zeta^{3^{1+2\cdot0}} + \zeta^{3^{1+2\cdot1}} + \zeta^{3^{1+2\cdot2}} + \zeta^{3^{1+2\cdot3}} + \zeta^{3^{1+2\cdot4}} + \zeta^{3^{1+2\cdot5}} + \zeta^{3^{1+2\cdot6}} + \zeta^{3^{1+2\cdot7}}\\ &= \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6.\end{aligned}$$

We form those sums of pairs of η's that yield an η from the previous step. Here there is only one pair, and the sum is given by

$$\eta_0 + \eta_1 = -1.$$

Next we form the elements $\eta^{(t)}$, remembering that for $t > 0$, $\eta^{(t)}$ is the η_r in which ζ^t occurs. Then $\eta^{(0)} = 2$,

$$\begin{aligned}\eta^{(1)} = \eta^{(9)} = \eta^{(13)} = \eta^{(15)} = \eta^{(16)} = \eta^{(8)} = \eta^{(4)} = \eta^{(2)} = \eta_0,\\ \eta^{(3)} = \eta^{(10)} = \eta^{(5)} = \eta^{(11)} = \eta^{(14)} = \eta^{(7)} = \eta^{(12)} = \eta^{(6)} = \eta_1.\end{aligned}$$

To compute $\eta_0\eta_1$ by means of Gauss's product formula, we use $\eta_0 = \eta^{(1)}$ and $\eta_1 = \eta^{(3)}$. Then

$$\eta_0\eta_1 = \eta^{(1)}\eta^{(3)} = \eta^{(4)} + \eta^{(11)} + \eta^{(6)} + \eta^{(12)} + \eta^{(15)} + \eta^{(8)} + \eta^{(13)} + \eta^{(7)},$$

the indices on the right side being the indices for η_1 plus one. Resubstituting in terms of η_0 and η_1, we obtain

$$\eta_0\eta_1 = 4\eta_0 + 4\eta_1 = -4.$$

Therefore η_0 and η_1 are the roots of the quadratic equation

$$x^2 + x - 4 = 0, \qquad \text{namely } \tfrac{1}{2}(-1 \pm \sqrt{17}\,).$$

Deciding which root is η_0 and which is η_1 involves looking at signs. The two roots of the quadratic equation are of opposite sign. Since

$$\begin{aligned}\eta_0 &= (\zeta^1 + \zeta^{-1}) + (\zeta^2 + \zeta^{-2}) + (\zeta^4 + \zeta^{-4}) + (\zeta^8 + \zeta^{-8})\\ &= 2\big(\cos(2\pi/17) + \cos(4\pi/17) + \cos(8\pi/17) + \cos(16\pi/17)\big)\\ &> 2\big(\tfrac{1}{2} + \tfrac{1}{2} + 0 + (-1)\big) = 0,\end{aligned}$$

[13] The discussion of this example closely follows that in Van der Waerden, Vol. I, Section 54.

η_0 is the positive root, and we have

$$\eta_0 = \tfrac{1}{2}(-1 + \sqrt{17}) \qquad \text{and} \qquad \eta_1 = \tfrac{1}{2}(-1 - \sqrt{17}).$$

For $k = 4$, the 4 periods have 4 terms each, and

$$\begin{aligned}
\xi_0 &= \zeta^{3^{0+4\cdot0}} + \zeta^{3^{0+4\cdot1}} + \zeta^{3^{0+4\cdot2}} + \zeta^{3^{0+4\cdot3}} = \zeta^1 + \zeta^{13} + \zeta^{16} + \zeta^4,\\
\xi_1 &= \zeta^{3^{1+4\cdot0}} + \zeta^{3^{1+4\cdot1}} + \zeta^{3^{1+4\cdot2}} + \zeta^{3^{1+4\cdot3}} = \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12},\\
\xi_2 &= \zeta^{3^{2+4\cdot0}} + \zeta^{3^{2+4\cdot1}} + \zeta^{3^{2+4\cdot2}} + \zeta^{3^{2+4\cdot3}} = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2,\\
\xi_3 &= \zeta^{3^{3+4\cdot0}} + \zeta^{3^{3+4\cdot1}} + \zeta^{3^{3+4\cdot2}} + \zeta^{3^{3+4\cdot3}} = \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6.
\end{aligned}$$

The sums of pairs of these that yield η's are

$$\begin{aligned}
\xi_0 + \xi_2 &= \eta_0\\
\xi_1 + \xi_3 &= \eta_1.
\end{aligned}$$

We can read off superscripted ξ's from the exponents on the right sides of the formulas for $\xi_0, \dots, \xi_3$, and the results are

$$\begin{aligned}
\xi^{(1)} = \xi^{(13)} = \xi^{(16)} = \xi^{(4)} &= \xi_0,\\
\xi^{(3)} = \xi^{(5)} = \xi^{(14)} = \xi^{(12)} &= \xi_1,\\
\xi^{(9)} = \xi^{(15)} = \xi^{(8)} = \xi^{(2)} &= \xi_2,\\
\xi^{(10)} = \xi^{(11)} = \xi^{(7)} = \xi^{(6)} &= \xi_3.
\end{aligned}$$

Then the relevant products are

$$\begin{aligned}
\xi_0\xi_2 = \xi^{(1)}\xi^{(9)} &= \xi^{(10)} + \xi^{(16)} + \xi^{(9)} + \xi^{(3)} = \xi_3 + \xi_0 + \xi_2 + \xi_1 = -1,\\
\xi_1\xi_3 = \xi^{(3)}\xi^{(6)} &= \xi^{(13)} + \xi^{(14)} + \xi^{(10)} + \xi^{(9)} = \xi_0 + \xi_1 + \xi_3 + \xi_2 = -1.
\end{aligned}$$

Thus ξ_0 and ξ_2 are the roots of the quadratic equation

$$y^2 - \eta_0 y - 1 = 0,$$

while ξ_1 and ξ_3 are the roots of the quadratic equation

$$y^2 - \eta_1 y - 1 = 0.$$

Since $\xi_0\xi_2$ and $\xi_1\xi_3$ are negative, these equations each have roots of opposite sign. We observe that $\xi_0 = 2\big(\cos(2\pi/17) + \cos(8\pi/17)\big) > 0$ and that $\xi_3 = 2\big(\cos(14\pi/17) + \cos(12\pi/17)\big) < 0$, and we conclude that the signs are

$$\begin{aligned}
\xi_0 > 0 \quad &\text{and} \quad \xi_2 < 0,\\
\xi_1 > 0 \quad &\text{and} \quad \xi_3 < 0.
\end{aligned}$$

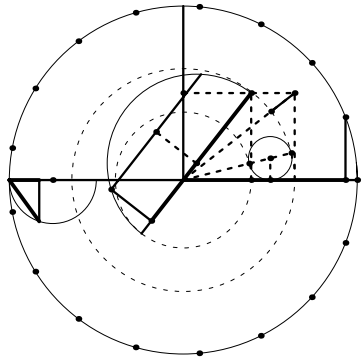


FIGURE 9.4. Construction of a regular 17-gon. The small circle has center $\left(\frac{1}{2}, \frac{1}{8}\right)$ and radius $\frac{1}{8}$. Two circles are drawn tangent to it with center $(0, 0)$; their radii are $\eta_0/4$ and $|\eta_1|/4$. Their x intercepts and height $\frac{1}{2}$ determine the dashed box. The diameter of the large solid semicircle is $\xi_0/2$, and its heavy part is $\lambda_0/2$. The separate semicircle at the left constructs $\sqrt{\xi_1/4}$ from $\xi_1/2$, and the chord in the large semicircle is at distance $\sqrt{\xi_1/4}$ from the diameter.

For $k = 8$, the 8 periods have 2 terms each, and the two with sum ξ_0 are

$$\lambda_0 = \zeta^{3^{0+8\cdot 0}} + \zeta^{3^{0+8\cdot 1}} = \zeta^1 + \zeta^{16},$$
$$\lambda_4 = \zeta^{3^{4+8\cdot 0}} + \zeta^{3^{4+8\cdot 1}} = \zeta^{13} + \zeta^4.$$

Their sum and their product are given by

$$\lambda_0 + \lambda_4 = \xi_0,$$
$$\lambda_0\lambda_4 = \zeta^{14} + \zeta^5 + \zeta^{12} + \zeta^3 = \xi_1.$$

Thus λ_0 and λ_4 are the roots of the quadratic equation

$$z^2 - \xi_0 z + \xi_1 = 0.$$

Since $\lambda_0 = 2\cos(2\pi/17) > 2\cos(8\pi/17) = \lambda_4$, λ_0 is the larger of the two roots of the equation.

In summary, we have successively defined

$$\eta_0 = \tfrac{1}{2}\big(-1 + \sqrt{17}\big) \quad \text{and} \quad \eta_1 = \tfrac{1}{2}\big(-1 - \sqrt{17}\big),$$
$$\xi_0 = \tfrac{1}{2}\big(\eta_0 + \sqrt{\eta_0^2 + 4}\big) \quad \text{and} \quad \xi_2 = \tfrac{1}{2}\big(\eta_0 - \sqrt{\eta_0^2 + 4}\big),$$
$$\xi_1 = \tfrac{1}{2}\big(\eta_1 + \sqrt{\eta_1^2 + 4}\big) \quad \text{and} \quad \xi_3 = \tfrac{1}{2}\big(\eta_1 - \sqrt{\eta_1^2 + 4}\big),$$
$$\lambda_0 = \tfrac{1}{2}\big(\xi_0 + \sqrt{\xi_0^2 - 4\xi_1}\big).$$

Pure Mathematical Physics

Since $\lambda_0 = 2\cos(2\pi/17)$, these formulas explicitly point to how to construct a regular 17-gon. See Figure 9.4.

13. Solution of Certain Polynomial Equations with Solvable Galois Group

In this section we investigate what specific information can be deduced about a finite Galois extension in characteristic 0 when the Galois group is solvable. The tool is a precursor of modern harmonic analysis[14] known as "Lagrange resolvents." The argument of the previous section could be regarded as an instance of applying the theory of Lagrange resolvents, but Lagrange resolvents give only the simpler formulas of the previous section, not the Gauss product formula.

Proposition 9.47. Let $\mathbb{K}$ be a finite normal extension of a field $\Bbbk$ of characteristic 0, suppose that $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is cyclic of order n with σ as a generator, and suppose that $X^n - 1$ splits in $\Bbbk$. Fix a generator σ of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ and a primitive n^{th} root ω of 1 in $\Bbbk$. For $0 \le r < n$, define $\Bbbk$ linear maps $E_r : \mathbb{K} \to \mathbb{K}$ by

$$E_r x = n^{-1} \sum_{k \bmod n} \omega^{-kr} \sigma^k x \qquad \text{for } x \in \mathbb{K}.$$

Then

(a) $E_r E_s$ equals E_s if $r = s$ and equals 0 if $r \not\equiv s \bmod n$, so that the E_r's are commuting projection operators whose images are linearly independent,
(b) $\sum_{r \bmod n} E_r = I$, so that the direct sum of the images of the E_r's is all of $\mathbb{K}$,
(c) $\sigma(x) = \omega^r x$ for all r and for all x in image E_r,
(d) image $E_0 = \Bbbk$.

REMARKS. The integers k and r depend only on their values modulo n, and the summation indices "$k \bmod n$" and "$r \bmod n$" are to be interpreted accordingly. The operators E_r are known classically as **Lagrange resolvents**, apart from the constant n^{-1}. The proposition says that the $\Bbbk$ linear map σ has a basis of eigenvectors, that the eigenvalues are a subset of the powers ω^r, and that each E_r is the projection operator on the eigenspace for the eigenvalue ω^r along the sum of the remaining eigenspaces.

[14]Lagrange resolvents give a certain specific Fourier decomposition relative to a cyclic group. Similar formulas apply whenever a cyclic group acts linearly on a vector space over $\Bbbk$ and the relevant roots of 1 lie in $\Bbbk$. For the corresponding decomposition of a vector space over $\mathbb{C}$ when a finite group G acts linearly, see Problems 47–52 at the end of Chapter VII. The decomposition in those problems can be seen to work for any field $\Bbbk$ of characteristic 0 for which the values of all irreducible characters of G lie in $\Bbbk$. The values of the characters are sums of certain roots of 1, and thus it is enough that $\Bbbk$ contain a certain finite set of roots of 1.

Pure Mathematical Physics

PROOF. For x in $\mathbb{K}$, we compute

$$\begin{aligned} E_r E_s x &= n^{-2} \sum_{k \bmod n} \omega^{-kr} \sigma^k \Big(\sum_{l \bmod n} \omega^{-ls} \sigma^l x \Big) \\ &= n^{-2} \sum_{k \bmod n} \sum_{m \bmod n} \omega^{-kr} \sigma^k \omega^{-ms+ks} \sigma^{m-k} x \\ &= n^{-2} \sum_{m \bmod n} \Big(\sum_{k \bmod n} \omega^{k(s-r)} \Big) \omega^{-ms} \sigma^m x. \end{aligned}$$

The expression in parentheses on the right side is the sum of a finite geometric series. If $s \equiv r \bmod n$, then every term in the sum is 1, and the sum is n. If $s \not\equiv r \bmod n$, then the sum is $\frac{1-\omega^{n(s-r)}}{1-\omega^{s-r}} = 0$. Thus (a) follows.

Next we calculate

$$\sum_{r \bmod n} E_r x = \sum_{r \bmod n} n^{-1} \sum_{k \bmod n} \omega^{-kr} \sigma^k x = \sum_{k \bmod n} n^{-1} \Big(\sum_{r \bmod n} \omega^{-kr} \Big) \sigma^k x.$$

As in the previous paragraph, the sum in parentheses is n if $k = 0$ and it is 0 if $k \not\equiv 0 \bmod n$. Therefore only the $k = 0$ term on the right side contributes, and the right side simplifies to x. This proves (b).

The computation

$$\begin{aligned} \sigma(E_r x) &= n^{-1} \sum_{k \bmod n} \omega^{-kr} \sigma^{k+1} x \\ &= n^{-1} \sum_{l \bmod n} \omega^{(-l+1)r} \sigma^l x \\ &= \omega^r n^{-1} \sum_{l \bmod n} \omega^{-lr} \sigma^l x = \omega^r E_r x \end{aligned}$$

shows that $\sigma(y) = \omega^r y$ for every y of the form $E_r x$, and these y's are the members of the image of E_r. This proves (c).

Combining (b) and (c), we see that $\sigma(x) = x$ if and only if x is in image E_0. Since $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is cyclic, the members of $\mathbb{K}$ fixed by σ are the members fixed by the Galois group, and these are the members of $\Bbbk$ by Proposition 9.35d. This proves (d). □

Corollary 9.48. Let $\mathbb{K}$ be a finite normal extension of a field $\Bbbk$ of characteristic 0, suppose that $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is cyclic of prime order p, and suppose that $X^p - 1$ splits in $\Bbbk$. Then there exist a in $\Bbbk$ and x in $\mathbb{K}$ such that $x^p = a$ and $\mathbb{K} = \Bbbk(x)$.

REMARKS. In other words, a finite normal extension field in characteristic 0 with Galois group cyclic of prime order p is necessarily obtained by adjoining a p^{th} root of some element of the base field, provided that the base field contains all the p^{th} roots of 1. Once the extension field contains one p^{th} root of an element of the base field, it has to contain all p^{th} roots, since the base field by assumption contains a full complement of p^{th} roots of 1.

PROOF. We apply Proposition 9.47 with $n = p$. Since $[\mathbb{K} : \Bbbk] = p > 1$, (d) shows that E_0 is not the identity. By (b), some E_r with $r \neq 0$ is not the 0 operator. Let x be a nonzero element in image E_r. Since the generator σ of the Galois group is a field automorphism, $\sigma(x^p) = \sigma(x)^p = (\omega^r x)^p = \omega^{rp} x^p = x^p$. Since x^p is fixed by the Galois group, x^p lies in $\Bbbk$. Then the element $a = x^p$ has the property that $x^p = a$ and $\mathbb{K} \supseteq \Bbbk(x) \supsetneqq \Bbbk$. Since $[\mathbb{K} : \Bbbk]$ is prime, Corollary 9.7 shows that there are no intermediate fields between $\mathbb{K}$ and $\mathbb{K}$. Therefore $\mathbb{K} = \Bbbk(x)$. □

We shall apply Corollary 9.48 to prove the converse statement in Theorem 9.44—that solvability of the Galois group for a polynomial equation in characteristic 0 implies that the solutions of the equation are expressible in terms of radicals and the base field. We begin with a lemma that handles a special case.

Lemma 9.49. Let $\Bbbk$ be a field of characteristic 0, let $n > 0$ be an integer, and let $\mathbb{K}$ be a splitting field for $\prod_{r=1}^{n} (X^r - 1)$ over $\Bbbk$. Then $\mathbb{K}/\Bbbk$ is a Galois extension, the Galois group of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is abelian, and $\mathbb{K}$ has a root tower over $\Bbbk$.

PROOF. Being a splitting field in characteristic 0, $\mathbb{K}$ is a finite Galois extension of $\Bbbk$. For $1 \leq r \leq n$, let ω_r be a primitive r^{th} root of 1 in $\mathbb{K}$. The primitive r^{th} roots of 1 are parametrized by the group $(\mathbb{Z}/r\mathbb{Z})^\times$ once some ω_r is specified, the parametrization being $k \mapsto \omega_r^k$. If σ is in $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, then $\sigma(\omega_r) = \omega_r^k$ for some such k. This correspondence respects multiplication in $(\mathbb{Z}/r\mathbb{Z})^\times$ since if $\sigma(\omega_r) = \omega_r^k$ and $\sigma'(\omega_r) = \omega_r^l$, then $\sigma'(\sigma(\omega_r)) = \sigma'(\omega_r^k) = \sigma'(\omega_r)^k = \omega_r^{kl}$. Thus for each r, we have a homomorphism of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ into the abelian group $(\mathbb{Z}/r\mathbb{Z})^\times$. Putting these homomorphisms together as r varies and using the fact that the ω_r's generate $\mathbb{K}$ over $\Bbbk$, we obtain a one-one homomorphism of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ into the abelian group $\prod_{r=1}^{n} (\mathbb{Z}/r\mathbb{Z})^\times$. Consequently $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is isomorphic to a subgroup of an abelian group and is abelian.

It follows from Corollary 9.39 that every extension of intermediate fields is Galois and has abelian Galois group. For $1 \leq r \leq n$, we introduce the intermediate field $\mathbb{K}_r = \Bbbk(\omega_1, \omega_2, \ldots, \omega_r)$. Here $\mathbb{K}_1 = \Bbbk(1) = \Bbbk$. For $1 < r < n$, $\mathbb{K}_r$ is generated as a vector space over $\mathbb{K}_{r-1}$ by $\omega_r, \omega_r^2, \ldots, \omega_r^{r-1}$ since $\sum_{k=0}^{r-1} \omega_r^k = 0$ for $r > 1$, and thus $[\mathbb{K}_r : \mathbb{K}_{r-1}] \leq r - 1$. Since $\mathrm{Gal}(\mathbb{K}_r/\mathbb{K}_{r-1})$ is abelian, it has a composition series whose consecutive quotients are cyclic of prime order, the prime order necessarily being $\leq [\mathbb{K}_r : \mathbb{K}_{r-1}] \leq r - 1$. Applying Galois theory, form the chain of intermediate extensions between $\mathbb{K}_{r-1}$ and $\mathbb{K}_r$. The degree of each extension is some prime p with $p \leq r - 1$, the prime depending on the two fields in the chain. The p^{th} roots of unity are in the smaller of any two consecutive fields because they are in $\mathbb{K}_{r-1}$. By Corollary 9.48, such a degree-p extension between $\mathbb{K}_{r-1}$ and $\mathbb{K}_r$ is generated by the smaller field and the p^{th} root of an element in the smaller field. Since $\mathbb{K}_1 = \Bbbk$, we see inductively that $\mathbb{K}_r$ has a root tower over $\mathbb{K}_{r-1}$ for each r. Since $\mathbb{K} = \mathbb{K}_n$, $\mathbb{K}$ has a root tower over $\Bbbk$. □

Pure Mathematical Physics

PROOF OF SUFFICIENCY IN THEOREM 9.44 THAT $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ BE SOLVABLE. Let $F(X)$ be in $\Bbbk[X]$, and suppose that $\mathbb{K}$ is a splitting field of $F(X)$ over $\Bbbk$. Under the assumption that $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is solvable, we are to prove that there exists a finite extension $\mathbb{K}'$ of $\mathbb{K}$ having a root tower.

Since $G = \mathrm{Gal}(\mathbb{K}/\Bbbk)$ is solvable, we can find a finite sequence of subgroups of G, each normal in the next larger one, such that the quotient of any consecutive pair is cyclic of prime order. We write

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_{k-1} \supseteq H_k = \{1\}$$

with H_j/H_{j+1} cyclic of prime order p_j for $0 \le j < k$. Let

$$\Bbbk = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{K}_{k-1} \subseteq \mathbb{K}_k = \mathbb{K}$$

be the corresponding sequence of intermediate fields given by the Fundamental Theorem of Galois Theory (Theorem 9.38). Here $\mathbb{K}_j = \mathbb{K}^{H_j}$, and $H_j = \mathrm{Gal}(\mathbb{K}/\mathbb{K}_j)$.

According to Corollary 9.39, $\mathbb{K}_{j+1}$ is a normal extension of $\mathbb{K}_j$ if and only if $\mathrm{Gal}(\mathbb{K}/\mathbb{K}_{j+1})$ is a normal subgroup of $\mathrm{Gal}(\mathbb{K}/\mathbb{K}_j)$, and in this case we have a group isomorphism $\mathrm{Gal}(\mathbb{K}/\mathbb{K}_j)\big/\mathrm{Gal}(\mathbb{K}/\mathbb{K}_{j+1}) \cong \mathrm{Gal}(\mathbb{K}_{j+1}/\mathbb{K}_j)$. Since H_{j+1} is a normal subgroup of H_j with quotient cyclic of order p_j, it follows that $\mathbb{K}_{j+1}/\mathbb{K}_j$ is indeed normal and the Galois group is cyclic of order p_j.

Let us use Theorem 9.22 to regard $\mathbb{K}$ as lying in a fixed algebraic closure $\overline{\mathbb{K}}'$. Let n be the product of all the primes p_j, and let $\mathbb{K}'_0$ be the splitting field over $\Bbbk$ for $\prod_{r=1}^{n}(X^r - 1)$ within $\overline{\mathbb{K}}'$. For $1 \le j \le k$, let $\mathbb{K}'_j$ be the subfield of $\overline{\mathbb{K}}'$ generated by $\mathbb{K}_j$ and $\mathbb{K}'_0$. We define $\mathbb{K}' = \mathbb{K}'_k$. Then we have

$$\Bbbk \subseteq \mathbb{K}'_0 \subseteq \mathbb{K}'_1 \subseteq \cdots \subseteq \mathbb{K}'_{k-1} \subseteq \mathbb{K}'_k = \mathbb{K}'.$$

Lemma 9.49 shows that $\mathbb{K}'_0$ has a root tower over $\mathbb{K}'$. To complete the proof, it is enough to show for each $j \ge 0$ that either $\mathbb{K}'_{j+1} = \mathbb{K}'_j$ or else $[\mathbb{K}'_{j+1} : \mathbb{K}'_j] = p_j$ and $\mathbb{K}'_{j+1}$ is generated by $\mathbb{K}'_j$ and the p_j^{th} root of some member of $\mathbb{K}'_j$.

For each $j \ge 0$, suppose that $\mathbb{K}_{j+1} = \mathbb{K}_j(x_j)$. Let $F_j(X)$ be the minimal polynomial of x_j over $\mathbb{K}_j$. Since $\mathbb{K}_{j+1}/\mathbb{K}_j$ is normal, $\mathbb{K}_{j+1}$ is the splitting field of $F_j(X)$ over $\mathbb{K}_j$. Then $\mathbb{K}'_{j+1} = \mathbb{K}'_j(x_j)$ is the splitting field of $F_j(X)\prod_{r=1}^{n}(X^r - 1)$ over $\mathbb{K}'_j$, and consequently $\mathbb{K}'_{j+1}/\mathbb{K}'_j$ is a normal extension. If g is in $\mathrm{Gal}(\mathbb{K}'_{j+1}/\mathbb{K}'_j)$, then g sends x_j into a root of $F_j(X)$ and is determined by this root. The restriction $g\big|_{\mathbb{K}_{j+1}}$ therefore carries $\mathbb{K}_{j+1}$ into itself and is in $\mathrm{Gal}(\mathbb{K}_{j+1}/\mathbb{K}_j)$. Since g is determined by $g(x_j)$, the group homomorphism $g \mapsto g\big|_{\mathbb{K}_{j+1}}$ is one-one. The image of this homomorphism must be a subgroup of $\mathrm{Gal}(\mathbb{K}_{j+1}/\mathbb{K}_j)$ and therefore must be trivial or have p_j elements. In the first case, $\mathbb{K}'_{j+1} = \mathbb{K}'_j$, and in the second case, $[\mathbb{K}'_{j+1} : \mathbb{K}'_j] = p_j$. In the latter case, $\mathbb{K}'_j$ contains all p_j of the p_j^{th} roots of 1 since these roots of 1 are in $\mathbb{K}'_0$; by Corollary 9.48, $\mathbb{K}'_{j+1}$ is generated by $\mathbb{K}'_j$ and a p_j^{th} root of some member of $\mathbb{K}'_j$. This completes the proof. □

We turn now to apply our methods to irreducible cubics over a field $\Bbbk$ of characteristic 0. In effect we shall derive Cardan's formula,[15] which was mentioned at the beginning of Section 11.

The Galois group of a splitting field of a cubic polynomial has to be a subgroup of the symmetric group $\mathfrak{S}_3$, and irreducibility of the cubic implies that the Galois group has to contain a 3-cycle. Therefore the Galois group has to be either $\mathfrak{S}_3$ or the alternating group $\mathfrak{A}_3 \cong C_3$.

Let the cubic be $X^3+a_2X^2+a_1X+a_0$, the coefficients being in $\Bbbk$. Substituting $X = Z - \frac{1}{3}a_2$ converts the polynomial into

$$(Z - \tfrac{1}{3}a_2)^3 + a_2(Z - \tfrac{1}{3}a_2)^2 + a_1(Z - \tfrac{1}{3}a_2) + a_0 \\ = Z^3 + (a_1 - \tfrac{1}{3}a_2^2)Z + (a_0 - \tfrac{1}{3}a_1a_2 + \tfrac{2}{27}a_2^3),$$

and therefore we can assume whenever convenient that the given polynomial has $a_2 = 0$.

Suppose for the moment that the Galois group is $G = \mathfrak{S}_3$. A composition series is

$$G = \mathfrak{S}_3 \supseteq \mathfrak{A}_3 \supseteq \{1\},$$

and we can write the corresponding sequence of fixed fields as

$$\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K},$$

where $\mathbb{K}$ is the splitting field and $\mathbb{L}$ is $\mathbb{K}^{\mathfrak{A}_3}$. The dimensions satisfy $[\mathbb{L} : \Bbbk] = 2$ and $[\mathbb{K} : \mathbb{L}] = 3$.

Let the roots in $\mathbb{K}$ of the given cubic be r_1, r_2, r_3. Since G is solvable, Theorem 9.44 tells us that the roots are expressible in terms of radicals and members of $\Bbbk$. To derive explicit formulas for the roots, the idea is to use a two-step process with Lagrange resolvents, arguing as in the proof of Corollary 9.48 at each step.

The first step involves passing from $\Bbbk$ to $\mathbb{L}$. The square roots of 1 are already in $\Bbbk$, and $\mathbb{L}$ is to be obtained from $\Bbbk$ by adjoining one of the square roots of some element of $\Bbbk$. In Proposition 9.47 the Galois group $\mathrm{Gal}(\mathbb{L}/\Bbbk)$ is a 2-element quotient group, the sum is over members of the quotient group, and the element x is in $\mathbb{L}$. It is a little more convenient to pull the sum back to one over the 6-element symmetric group, taking ω to be the sign function on $\mathfrak{S}_3$ and taking x to be any element of $\mathbb{K}$. The formulas for the projection operators E_0 and E_1 are then

$$E_0x = \tfrac{1}{6}\sum_{\sigma\in\mathfrak{S}_3} \sigma(x),$$
$$E_1x = \tfrac{1}{6}\sum_{\sigma\in\mathfrak{S}_3} (\operatorname{sgn}\sigma)\sigma(x),$$

[15] We discuss only Cardan's cubic formula, omitting any discussion of the corresponding quartic formula, which often bears Cardan's name and which can be handled with the same techniques. See Van der Waerden, Vol. I, Section 58, for details.

with x in $\mathbb{K}$, and the proof of Corollary 9.48 tells us to adjoin to $\Bbbk$ the square root of any element of image E_1, i.e., any element with $\sigma(x) = (\operatorname{sgn} x)x$ for all σ in $\mathfrak{S}_3$.

The only elements of $\mathbb{K}$ for which we have good control of the action of the Galois group, apart from the elements of $\Bbbk$, are the elements that are expressed directly in terms of the roots r_1, r_2, r_3 of the polynomial. By renumbering the roots if necessary, we may assume that the roots are permuted by $\mathfrak{S}_3$ according to their subscripts. An example of a polynomial function of r_1, r_2, r_3 that transforms according to the sign of the permutation played a role in Section I.4 in defining the sign of a permutation. It is the **difference product** of the polynomial, namely

$$\prod_{1 \le i < j \le 3} (r_j - r_i).$$

This is a square root of the **discriminant** D of the polynomial, which is given by

$$D = \prod_{1 \le i < j \le 3} (r_j - r_i)^2.$$

We shall compute D in terms of the coefficients of the cubic shortly. In the meantime, the proof of Corollary 9.48 thus tells us that $\mathbb{L} = \Bbbk(\sqrt{D}\,)$. Here $\sqrt{D}$ is given by

$$\begin{aligned}\sqrt{D} &= (r_3 - r_2)(r_3 - r_1)(r_2 - r_1)\\ &= (r_1 r_2^2 + r_2 r_3^2 + r_3 r_1^2) - (r_1^2 r_2 + r_2^2 r_3 + r_3^2 r_1).\end{aligned}$$

The second step is to pass from $\mathbb{L}$ to $\mathbb{K}$. Corollary 9.48 says to expect $\mathbb{K}$ to be obtained by adjoining the cube root of something if the cube roots of 1 are already present in $\mathbb{L}$. The proof of the second half of Theorem 9.44, which follows Corollary 9.48, indicates how we can incorporate the cube roots of 1 into the fields in order to have a root tower. What we can do is to replace $\Bbbk$ at the start by a splitting field for $\prod_{1 \le r \le 3} (X^r - 1)$. Since ± 1 are already in $\Bbbk$, we are to adjoin the nontrivial cube roots of 1, i.e., the roots of $X^2 + X + 1$, if they are not already present. In other words, what we do is replace $\Bbbk$ at the start by $\Bbbk(\sqrt{-3}\,)$. Changing notation, we assume that $\sqrt{-3}$ lies in $\Bbbk$ from the outset.

We can now use Lagrange resolvents. Let σ be the generator (1 2 3) of $\mathfrak{A}_3$, sending r_1 to r_2, r_2 to r_3, and r_3 to r_1. Let $\omega = \frac{1}{2}(-1 + \sqrt{-3}\,)$ be a primitive cube root of 1. Then we have

$$\begin{aligned}E_0 x &= \tfrac{1}{3}(x + \sigma x + \sigma^2 x),\\ E_1 x &= \tfrac{1}{3}(x + \omega^{-1}\sigma x + \omega^{-2}\sigma^2 x),\\ E_2 x &= \tfrac{1}{3}(x + \omega^{-2}\sigma x + \omega^{-1}\sigma^2 x).\end{aligned}$$

Again we can use any x, but the roots of the cubic are the simplest nontrivial elements for which we know the action of σ. Corollary 9.48 shows that $\mathbb{K} = \mathbb{L}(E_1x)$ if $E_1x \neq 0$. Proposition 9.47 says that $(E_1x)^3$ is fixed by σ, and it therefore lies in $\mathbb{L}$. Hence $\mathbb{K}$ is identified as obtained from $\mathbb{L}$ by adjoining a cube root of the element $(E_1x)^3$ of $\mathbb{L}$.

Taking $x = r_1$, we have $\sigma x = r_2$ and $\sigma^2 x = r_3$. Also, $\omega^{\pm 1} = \frac{1}{2}(-1 \pm \sqrt{-3}\,)$. Using the formula for E_1x and substituting for $\sqrt{D}$ and $\omega^{\pm 1}$ then gives

$$\begin{aligned}(3E_1r_1)^3 &= r_1^3 + r_2^3 + r_3^2 + 6r_1r_2r_3 \\ &\quad + 3\omega^{-1}(r_1^2r_2 + r_2^2r_3 + r_3^2r_1) + 3\omega(r_1r_2^2 + r_2r_3^2 + r_3r_1^2) \\ &= \sum_i r_i^3 + 6r_1r_2r_3 - \tfrac{3}{2}\sum_{i\neq j} r_i^2r_j + \tfrac{3}{2}\sqrt{-3}\sqrt{D}.\end{aligned}$$

To proceed further, we shall want to substitute expressions involving the coefficients of the cubic for the above symmetric expressions in the roots.[16] These expressions will be considerably simplified if we assume that the coefficient of X^2 in the cubic is 0. We know that this assumption involves no loss of generality. Thus we assume for the remainder of this section that the cubic is $X^3 + pX + q$. The relevant formulas relating the roots and the coefficients are

$$\begin{aligned}r_1 + r_2 + r_3 &= 0, \\ r_1r_2 + r_1r_3 + r_2r_3 &= p, \\ r_1r_2r_3 &= -q.\end{aligned}$$

Aiming for the right side of the displayed formula for $(3E_1r_1)^3$, we have

$$\begin{aligned}0 &= (r_1 + r_2 + r_3)^3 = \sum_i r_i^3 + 3\sum_{i\neq j} r_i^2r_j + 6r_1r_2r_3, \\ 0 &= (r_1 + r_2 + r_3)(r_1r_2 + r_1r_3 + r_2r_3) = -\tfrac{9}{2}\sum_{i\neq j} r_i^2r_j - \tfrac{27}{2}r_1r_2r_3, \\ -\tfrac{27}{2}q &= \tfrac{27}{2}r_1r_2r_3.\end{aligned}$$

Addition of these three lines and comparison with the expression for $3(E_1r_1)^3$ yields

$$-\tfrac{27}{2}q = \sum_i r_i^3 - \tfrac{3}{2}\sum_{i\neq j} r_i^2r_j + 6r_1r_2r_3 = (3E_1r_1)^3 - \tfrac{3}{2}\sqrt{-3}\sqrt{D}.$$

Consequently

$$(3E_1r_1)^3 = -\tfrac{27}{2}q + \tfrac{3}{2}\sqrt{-3}\sqrt{D}.$$

[16] Problems 36–39 at the end of Chapter VIII assure us that this rewriting is possible. For our derivation this assurance is not logically necessary, since we will be producing explicit formulas.

Similarly

$$(3E_2r_1)^3 = -\tfrac{27}{2}q - \tfrac{3}{2}\sqrt{-3}\sqrt{D}.$$

Since $3E_0r_1 = r_1 + r_2 + r_3 = 0$, we have expressions for E_0r_1, E_1r_1, and E_2r_1, apart from the choices of the cube roots. Proposition 9.47b says that we recover r_1 by addition: $r_1 = E_0r_1 + E_1r_1 + E_2r_1$. Thus we have found a root explicitly as soon as we sort out the ambiguity in the choices of cube roots and determine the value of D in terms of the coefficients p and q.

Theorem 9.50 (Cardan's formula). Let $\Bbbk$ be a field of characteristic 0 containing $\sqrt{-3}$, and let $X^3 + pX + q$ be an irreducible cubic in $\Bbbk[X]$. For this polynomial the discriminant D is given by

$$D = -4p^3 - 27q^2.$$

The Galois group of a splitting field of the cubic is $\mathfrak{S}_3$ if D is a nonsquare in $\Bbbk$ and is $\mathfrak{A}_3$ if D is a square in $\Bbbk$. In either case, fix a square root of D, denote it by $\sqrt{D}$, and let $\omega^{\pm1} = \frac{1}{2}(-1 \pm \sqrt{-3})$ be the primitive cube roots of 1. Then it is possible to determine cube roots of the form

$$3E_1r_1 = \sqrt[3]{-\tfrac{27}{2}\,q + \tfrac{3}{2}\sqrt{-3}\sqrt{D}} \quad \text{and} \quad 3E_2r_1 = \sqrt[3]{-\tfrac{27}{2}\,q - \tfrac{3}{2}\sqrt{-3}\sqrt{D}}$$

in such a way that their product is $(3E_1r_1)(3E_1r_2) = -3p$, and in this case the three roots of $X^3 + pX + q$ are given by

$$\begin{aligned} r_1 &= E_1r_1 + E_2r_1, \\ r_2 &= \omega E_1r_1 + \omega^2 E_2r_1, \\ r_3 &= \omega^2 E_1r_1 + \omega E_2r_1. \end{aligned}$$

PROOF. Define $\sigma_k = r_1^k + r_2^k + r_3^k$ for $1 \le k \le 4$. By inspection we have

$$\begin{pmatrix} 1 & 1 & 1 \\ r_1 & r_2 & r_3 \\ r_1^2 & r_2^2 & r_3^2 \end{pmatrix} \begin{pmatrix} 1 & r_1 & r_1^2 \\ 1 & r_2 & r_2^2 \\ 1 & r_3 & r_3^2 \end{pmatrix} = \begin{pmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix}.$$

Taking the determinant of both sides and applying Corollary 5.3, we obtain

$$D = \det \begin{pmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix} = 3\sigma_2\sigma_4 - \sigma_2^3 - 3\sigma_3^2.$$

The given cubic shows that $\sigma_1 = r_1 + r_2 + r_3 = 0$. For the other σ_i's, we have

$$\begin{aligned}
\sigma_2 = r_1^2 + r_2^2 + r_3^2 &= (r_1 + r_2 + r_3)^2 - 2(r_1r_2 + r_1r_3 + r_2r_3) = -2p,\\
\sigma_3 = r_1^3 + r_2^3 + r_3^3 &= (r_1 + r_2 + r_3)(r_1^2 + r_2^2 + r_3^2)\\
&\quad - (r_1^2r_2 + r_1^2r_3 + r_2^2r_1 + r_2^2r_3 + r_3^2r_1r_3^2r_2)\\
&= -(r_1 + r_2 + r_3)(r_1r_2 + r_1r_3 + r_2r_3) + 3r_1r_2r_3 = -3q,\\
\sigma_4 = r_1^4 + r_2^4 + r_3^4 &= (r_1^2 + r_2^2 + r_3^2)^2 - 2(r_1^2r_2^2 + r_1^2r_3^2 + r_2^2r_3^2)\\
&= (-2p)^2 - 2(r_1r_2 + r_1r_3 + r_2r_3)^2\\
&\quad + 4r_1r_2r_3(r_1 + r_2 + r_3) = (-2p)^2 - 2(p)^2 = 2p^2.
\end{aligned}$$

Substituting, we obtain $D = -12p^3 + 8p^3 - 27q^2 = -4p^3 - 27q^2$. This proves the formula for D. In particular, it confirms that D lies in $\Bbbk$.

The Galois group of the splitting field of the polynomial must be $\mathfrak{S}_3$ or $\mathfrak{A}_3$. If it is $\mathfrak{S}_3$, then we saw above that $\mathbb{L} = \Bbbk(\sqrt{D})$ and that $[\mathbb{L} : \Bbbk] = 2$. Hence D is a nonsquare in $\Bbbk$. If the Galois group is $\mathfrak{A}_3$, then $(r_3 - r_2)(r_3 - r_1)(r_2 - r_1)$ is fixed by the Galois group and lies in $\Bbbk$. The square of this element is D, and hence D is a square in $\Bbbk$.

With either Galois group the calculations with the cubic extension that precede the statement of the theorem are valid. If r_1 is one of the roots, then we know that

$$\begin{aligned}
r_1 &= E_0r_1 + E_1r_1 + E_2r_1 = E_1r_1 + E_2r_1,\\
(3E_1r_1)^3 &= -\tfrac{27}{2}q + \tfrac{3}{2}\sqrt{-3}\sqrt{D},\\
(3E_2r_1)^3 &= -\tfrac{27}{2}q - \tfrac{3}{2}\sqrt{-3}\sqrt{D}.
\end{aligned}$$

The uniqueness of simple extensions (Theorem 9.11) says that we can make any choice of cube root to determine $3E_1r_1$. Then

$$\begin{aligned}
(3E_1r_1)(3E_2r_1) &= (r_1 + \omega^{-1}\sigma r_1 + \omega^{-2}\sigma^2 r_1)(r_1 + \omega^{-2}\sigma r_1 + \omega^{-1}\sigma^2 r_1)\\
&= (r_1 + \omega^{-1}r_2 + \omega r_3)(r_1 + \omega r_2 + \omega^{-1}r_3)\\
&= (r_1^2 + r_2^2 + r_3^2) + (\omega + \omega^{-1})(r_1r_2 + r_1r_3 + r_2r_3)\\
&= (r_1^2 + r_2^2 + r_3^2) - (r_1r_2 + r_1r_3 + r_2r_3).
\end{aligned}$$

The first term on the right side we calculated in the first paragraph of the proof as $\sigma_2 = -2p$, and the second term gives $-p$. Thus $(3E_1r_1)(3E_2r_1) = -3p$ as asserted. Since σ operates on image E_1 as multiplication by ω and on image E_2 as multiplication by ω^2, the fact that $r_1 = E_1r_1 + E_2r_1$ implies that

$$r_2 = \sigma(r_1) \ = \omega E_1r_1 + \omega^2 E_2r_1$$

and

$$r_3 = \sigma^2(r_1) = \omega^2 E_1r_1 + \omega E_2r_1.$$

This completes the proof.

14. Proof That π Is Transcendental

In this section and the next three, we combine Galois theory with some of the ring theory in the second half of Chapter VIII. This combination will allow us to prove some striking theorems, see how Galois groups can be used effectively in practice, and develop some techniques for identifying Galois groups explicitly.

The present section is devoted to the proof of the following theorem.

Theorem 9.51 (Lindemann, 1882). The number π is transcendental over $\mathbb{Q}$.

The argument we give is based on that in a book by L. K. Hua.[17] For purposes of having a precise theorem, π is defined as the least positive real number such that $e^{\pi i} = -1$. In addition to Galois theory in the form of Proposition 9.35, the proof here will make use of a few facts about algebraic integers. Algebraic integers were defined in Section VIII.1 and again in Section VIII.9 (as well as in Section VII.4) as complex numbers that are roots of monic polynomials in $\mathbb{Z}[X]$. The algebraic integers form a ring by Corollary 8.38 (or alternatively by Lemma 7.30), the only algebraic integers in $\mathbb{Q}$ are the members of $\mathbb{Z}$ by Proposition 8.41 (or alternatively by Lemma 7.30), and any algebraic number x has the property that nx is an algebraic integer for some integer $n \neq 0$ by Proposition 8.42.

We begin with a lemma.

Lemma 9.52. Let $f(X)$ in $\mathbb{C}[X]$ be given by $f(X) = \sum_{k=0}^{n} a_k X^k$, and define $F(X)$ to be the sum of the derivatives of $f(X)$:

$$F(X) = \sum_{l=0}^{n} f^{(l)}(X).$$

If $Q(z)$ is defined as $Q(z) = F(0)e^z - F(z)$ for $z \in \mathbb{C}$, then $F(0) = \sum_{k=0}^{n} a_k k!$ and

$$|Q(z)| \le e^{|z|} \sum_{k=0}^{n} |a_k||z|^k.$$

PROOF. We calculate directly that

$$F(z) = \sum_{l=0}^{n} \sum_{k=l}^{n} \frac{a_k k!}{(k-l)!} z^{k-l} = \sum_{k=0}^{n} a_k \sum_{l=0}^{k} \frac{k!}{(k-l)!} z^{k-l} = \sum_{k=0}^{n} a_k \sum_{l=0}^{k} \frac{k!}{l!} z^l.$$

[17] *Introduction to Number Theory*, pp. 484–488. In the same pages Hua establishes the earlier theorem of Hermite that e is transcendental, using a related but simpler argument.

Pure Mathematical Physics

Evaluation at $z = 0$ gives $F(0) = \sum_{k=0}^{n} a_k k!$. Then

$$\begin{aligned}
|Q(z)| &\le \Big| \sum_{k=0}^{n} a_k \sum_{l=0}^{\infty} \frac{k!}{l!} z^l - \sum_{k=0}^{n} \sum_{l=0}^{k} \frac{k!}{l!} z^l \Big| \\
&= \Big| \sum_{k=0}^{n} a_k \sum_{l=k+1}^{\infty} \frac{k!}{l!} z^l \Big| \\
&\le \sum_{k=0}^{n} |a_k| \sum_{l=k+1}^{\infty} \frac{|z|^l}{(l-k)!} \qquad \text{since } \tbinom{l}{k}^{-1} \le 1 \\
&= \sum_{k=0}^{n} |a_k| |z|^k \sum_{m=1}^{\infty} \frac{|z|^m}{m!} \\
&\le e^{|z|} \sum_{k=0}^{n} |a_k| |z|^k .
\end{aligned}$$

PROOF OF THEOREM 9.51. Arguing by contradiction, suppose that π is algebraic over $\mathbb{Q}$, so that $\alpha = \pi i$ is algebraic over $\mathbb{Q}$ as well. Let $M(X)$ be the minimal polynomial of α over $\mathbb{Q}$, and let $\mathbb{K}$ be the splitting field of $M(X)$ in $\mathbb{C}$. This exists since $\mathbb{C}$ is algebraically closed. We write $\alpha_1, \dots, \alpha_m$ for the roots of $M(X)$ in $\mathbb{K}$, with $\alpha_1 = \alpha$. These are distinct algebraic numbers, and they are permuted by the Galois group, $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. What we shall show is that

$$R = \prod_{j=1}^{m} (1 + e^{\alpha_j}) \neq 0.$$

This will be a contradiction since $1 + e^{\alpha_1} = 0$ for $\alpha_1 = i\pi$.

We expand the product defining R, obtaining

$$R = 1 + \sum_{j} e^{\alpha_j} + \sum_{j,k} e^{\alpha_j + \alpha_k} + \cdots ,$$

Whenever one of the exponentials has total exponent 0, we lump that term with the constant 1. Otherwise we write the term as e^{β_l}, allowing repetitions among terms e^{β_l}. Thus

$$R = N + e^{\beta_1} + e^{\beta_2} + \cdots + e^{\beta_r},$$

with N an integer ≥ 1, with each $\beta_l \neq 0$, and with $N + r = 2^m$.

Each member of $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ permutes $\alpha_1, \dots, \alpha_m$, and it therefore permutes the β_l's that are single α_j's, permutes the β_l's that are the nonzero sums of two α_j's, permutes the β_l's that are the nonzero sums of three α_j's, and so on.

Choose an integer $a > 0$ such that $a\alpha_1, \dots, a\alpha_m$ are algebraic integers, let p be a prime number large enough to satisfy some conditions to be specified shortly, and define

$$f(X) = \frac{(aX)^{p-1}}{(p-1)!} \prod_{l=1}^{r} (aX - a\beta_l)^p = \sum_{k=0}^{n} a_k X^n .$$

Pure Mathematical Physics

The members σ of G act on $f(X)$ as usual by acting on the coefficients. Each β_l that is the nonzero sum of a certain number of α_j's is sent into another $\beta_{l'}$ of the same kind, and thus σ just permutes the factors of the product defining f, leaving $f(X)$ unchanged. The coefficients of $(p-1)!f(a^{-1}X)$ are algebraic integers in $\mathbb{K}$. Being fixed by G, they are in $\mathbb{Q}$ by Proposition 9.35d, and hence they are in $\mathbb{Z}$. Therefore

$$f(X) = \frac{A_{p-1}a^{p-1}X^{p-1} + A_p a^p X^p + \cdots}{(p-1)!}$$

with $A_{p-1}, A_p, \ldots$ in $\mathbb{Z}$. Since $A_{p-1} = \prod_{l=1}^{r}(-a\beta_l)^p$, we can arrange that p does not divide $A_{p-1}a^{p-1}$ by choosing p greater than a and greater than $\bigl|\prod_{l=1}^{r}(a\beta_l)\bigr|$. If we look at the l^{th} factor in the product defining $f(X)$, we see that $(X-\beta_l)^p$ divides $f(X)$ in $\mathbb{K}[X]$. Therefore we have further formulas for $f(X)$, namely

$$f(X) = \frac{\gamma_{p,l}(X-\beta_l)^p + \gamma_{p+1,l}(X-\beta_l)^{p+1} + \cdots}{(p-1)!} \qquad \text{for } 1 \le l \le r.$$

As in Lemma 9.52, we define

$$F(X) = \sum_{l=0}^{n} f^{(l)}(X) \qquad \text{and} \qquad Q(z) = F(0)e^z - F(z).$$

Then we have $F(0) = \sum_{k=0}^{n} a_k k!$. For $1 \le l \le r$, the definition of $Q(z)$ gives $F(0)e^{\beta_l} = F(\beta_l) + Q(\beta_l)$. Substituting from the definition of R, we obtain

$$F(0)R = F(0)\bigl(N + \sum_{l=1}^{r} e^{\beta_l}\bigr) = NF(0) + \sum_{l=1}^{r} F(\beta_l) + \sum_{l=1}^{r} Q(\beta_l). \qquad (*)$$

A further condition that we impose on the size of p is that $p > N$. Then the computation

$$NF(0) = N\sum_{k=0}^{n} a_k k! = N(A_{p-1}a^{p-1} + pA_p a^p + p(p+1)A_{p+1}a^{p+1} + \cdots)$$

and the properties of $A_{p-1}, A_p, \ldots$ together imply that $NF(0)$ is an integer and is not divisible by p.

Let us compute $F(\beta_l)$. The derivatives through order $p-1$ of $f(X)$ are 0 at β_l. For the p^{th} derivative we have

$$p\gamma_{p,l} = f^{(p)}(\beta_l) = pA_p a^p + \sum_{j\ge 1} \frac{(p+j)\cdots(j+1)}{(p-1)!} A_{p+j}a^{p+j}\beta_l^j.$$

The coefficient of $A_{p+j}a^{p+j}\beta_l^j$ inside the sum equals

$$\frac{(p+j)\cdots(j+1)j!p}{p(p-1)!j!} = p\binom{p+j}{j},$$

and thus

$$p\gamma_{p,l} = f^{(p)}(\beta_l) = a^p\big(pA_p + \sum_{j\ge1} p\tbinom{p+j}{j}A_{p+j}(a\beta_l)^j\big).$$

The higher-order derivatives are computed and simplified similarly. For the $(p+k)^{\text{th}}$ derivative with $k \ge 1$, we find that

$$\begin{aligned}(p+k)\cdots(p+1)p\gamma_{p+k,l} &= f^{(p+k)}(\beta_l)\\ &= a^{p+k}\big((p+k)\cdots(p+1)pA_{p+k} \qquad (**)\\ &\quad + \sum_{j\ge1}(p+k)\cdots(p+1)p\tbinom{p+j+k}{j}A_{p+j+k}(a\beta_l)^j\big).\end{aligned}$$

Put $C_{p+k} = \sum_{l=1}^r \gamma_{p+k,l}$. Summing the left and right members of $(**)$ over l gives

$$C_{p+k} = a^{p+k}\big(rA_{p+k} + \sum_{j\ge1}\tbinom{p+j+k}{j}A_{p+j+k}\sum_{j=1}^{l}(a\beta_l)^j\big).$$

The sum $\sum_{j=1}^l (a\beta_l)^j$ is an algebraic integer fixed by G, and it is therefore an integer. Consequently each C_{p+k} is an integer. Summing the left and middle members of $(**)$ over k and l gives

$$\sum_{l=1}^r F(\beta_l) = \sum_{k\ge0}(p+k)\cdots(p+1)pC_{p+k},$$

and this is an integer divisible by p.

Since $NF(0)$ is an integer not divisible by p, $NF(0) + \sum_{l=1}^r F(\beta_l)$ is an integer not divisible by p, and we have

$$\big|NF(0) + \sum_{l=1}^r F(\beta_l)\big| \ge 1.$$

In view of $(*)$, we will have a contradiction to $R = 0$ if we show that

$$\big|\sum_{l=1}^r Q(\beta_l)\big| < 1.$$

An easy argument by induction on m shows that if $\sum_{k=0}^m d_k z^k = \prod_{j=1}^s (z - c_j)$, then $\sum_{k=0}^m |d_k||z|^k \le \prod_{j=1}^s (|z| + |c_j|)$. Applying this observation to the sum and product defining $f(X)$ and using Lemma 9.52, we see that

$$e^{-|z|}|Q(z)| \le \sum_{k=0}^n |a_k||z|^k \le \frac{(a|z|)^{p-1}\prod_{l=1}^r (a|z| + a|\beta_l|)^p}{(p-1)!}.$$

Pure Mathematical Physics

For each fixed z, the right side is the $(p-1)^{\text{st}}$ term of the convergent series for an exponential function at an appropriate point, and hence the right side is less than $r^{-1}e^{-|z|}$ for p sufficiently large, p depending on z. Choosing p large enough to make the right side less than $r^{-1}e^{-|z|}$ for $z = \beta_1, \dots, \beta_l$ and summing over these z's, we obtain $\left|\sum_{l=1}^{r} Q(\beta_l)\right| < 1$, and we have arrived at the contradiction we anticipated. □

15. Norm and Trace

This is the second of four sections in which we combine Galois theory with some of the ring theory in the second half of Chapter VIII. We shall make use of a little more linear algebra than we have used thus far in this chapter, and we shall conclude the section by completing the proof of Theorem 8.54 concerning extensions of Dedekind domains.

Let $\Bbbk$ be a field, not necessarily of characteristic 0, and let $\mathbb{K}$ be a finite algebraic extension. We take advantage of the fact that $\mathbb{K}$ is a vector space over $\Bbbk$. If a is in $\mathbb{K}$, let us write $M(a)$ for the $\Bbbk$ linear mapping from $\mathbb{K}$ to $\mathbb{K}$ given by multiplication by a. The characteristic polynomial $\det(XI - M(a))$ is called the **field polynomial** of a and is a monic polynomial in $\Bbbk[X]$ of degree $[\mathbb{K} : \Bbbk]$. The **norm** and **trace** of a relative to $\mathbb{K}/\Bbbk$ are defined to be the determinant and trace of the linear mapping $M(a)$. In symbols,

$$N_{\mathbb{K}/\Bbbk}(a) = \det(M(a)),$$
$$\mathrm{Tr}_{\mathbb{K}/\Bbbk}(a) = \mathrm{Tr}(M(a)).$$

Both $N_{\mathbb{K}/\Bbbk}$ and $\mathrm{Tr}_{\mathbb{K}/\Bbbk}$ are functions from $\mathbb{K}$ to $\Bbbk$. If $n = [\mathbb{K} : \Bbbk]$, then $N_{\mathbb{K}/\Bbbk}(a)$ is $(-1)^n$ times the constant term of $\det(XI - M(a))$, and $\mathrm{Tr}_{\mathbb{K}/\Bbbk}(a)$ is minus the coefficient of X^{n-1}. The subscript $\mathbb{K}/\Bbbk$ may be omitted when there is no chance of ambiguity.

EXAMPLE. $\Bbbk = \mathbb{Q}$, $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, $a = \sqrt{2}$. If we use $\Gamma = (1, \sqrt{2})$ as an ordered basis of $\mathbb{K}$ over $\Bbbk$, then the matrix of $M(a)$ relative to Γ is $\begin{pmatrix} M(a) \\ \Gamma\Gamma \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$. Since characteristic polynomials are independent of the choice of basis, the field polynomial of a can be computed in this basis and is given by

$$\det \begin{pmatrix} XI - M(a) \\ \Gamma\Gamma \end{pmatrix} = \det \begin{pmatrix} X & -2 \\ -1 & X \end{pmatrix} = X^2 - 2.$$

We can read off the norm and trace as $N(a) = -2$ and $\mathrm{Tr}(a) = 0$.

Pure Mathematical Physics

Proposition 9.53. If $\mathbb{K}/\Bbbk$ is a finite extension of fields with $n = [\mathbb{K} : \Bbbk]$, then norms and traces relative to $\mathbb{K}/\Bbbk$ have the following properties:

(a) $N(ab) = N(a)N(b)$,
(b) $N(ca) = c^n N(a)$ for $c \in \Bbbk$,
(c) $N(1) = 1$, and consequently $N(c) = c^n$ for $c \in \Bbbk$,
(c) $\mathrm{Tr}(a + b) = \mathrm{Tr}(a) + \mathrm{Tr}(b)$,
(d) $\mathrm{Tr}(ca) = c\,\mathrm{Tr}(a)$ for $c \in \Bbbk$,
(e) $\mathrm{Tr}(1) = n$, and consequently $\mathrm{Tr}(c) = nc$ for $c \in \Bbbk$.

PROOF. Properties (a) and (b) follow from properties of the determinant in combination with the identities $M(ab) = M(a)M(b)$ and $M(ca) = cM(a)$. Properties (c) and (d) follow from properties of the trace in combination with the identities $M(a + b) = M(a) + M(b)$ and $M(ca) = cM(a)$. Since $M(1)$ is the identity, the norm and trace of 1 are 1 and n, respectively. The other conclusions in (c) and (e) are then consequences of this fact in combination with (b) and (d). □

Proposition 9.54. Let $\mathbb{K}/\Bbbk$ and $\mathbb{L}/\mathbb{K}$ be finite extensions of fields with $[\mathbb{K} : \Bbbk] = n$ and $[\mathbb{L} : \mathbb{K}] = m$, and let a be in $\mathbb{K}$. The element a acts by multiplication on $\mathbb{K}$ and also on $\mathbb{L}$, yielding $\Bbbk$ linear maps in each case that will be denoted by $M_{\mathbb{K}/\Bbbk}(a)$ and $M_{\mathbb{L}/\Bbbk}(a)$. Then in suitable ordered vector-space bases the matrix of $M_{\mathbb{L}/\Bbbk}(a)$ is block diagonal, each block being the matrix of $M_{\mathbb{K}/\Bbbk}(a)$.

PROOF. We choose the bases as in Theorem 7.6. Thus let $\Gamma = (\omega_1, \omega_2, \dots)$ be an ordered basis of $\mathbb{K}$ over $\Bbbk$, and let $\Delta = (\xi_1, \xi_2, \dots)$ be a basis of $\mathbb{L}$ over $\mathbb{K}$. Theorem 7.6 observes that the mn products $\xi_i\omega_j$ form a basis of $\mathbb{L}$ over $\Bbbk$, and we make this set into an ordered basis Ω by saying that $(i_1, j_1) < (i_2, j_2)$ if $i_1 < i_2$ or if $i_1 = i_2$ and $j_1 < j_2$. Let $M_{\mathbb{K}/\Bbbk}(a)\omega_j = \sum_l c_{lj}\omega_l$. Then

$$M_{\mathbb{L}/\Bbbk}(a)\xi_i\omega_j = \Big(\sum_{l=1}^{n} c_{lj}\omega_l\Big)\xi_i = \sum_{k=1}^{m}\sum_{l=1}^{n}(\delta_{ki}c_{lj})\xi_k\omega_l,$$

where δ_{ki} is 1 when $k = i$ and is 0 otherwise. The matrix $\left(\begin{smallmatrix} M_{\mathbb{L}/\Bbbk}(a) \\ \Omega\Omega \end{smallmatrix}\right)$ has $((k, l), (i, j))^{\text{th}}$ entry $\delta_{ki}c_{lj}$, and this is 0 unless the primary indices k and i are equal. Thus the matrix is block diagonal, the entries of the i^{th} diagonal block being c_{lj}. □

Corollary 9.55. Let $\mathbb{K}/\Bbbk$ and $\mathbb{L}/\mathbb{K}$ be finite extensions of fields with $[\mathbb{L} : \mathbb{K}] = m$, and let a be in $\mathbb{K}$. Let $M_{\mathbb{K}/\Bbbk}(a)$ and $M_{\mathbb{L}/\Bbbk}(a)$ denote multiplication by a on $\mathbb{K}$ and on $\mathbb{L}$, and let $F_{\mathbb{K}/\Bbbk}(X)$ and $F_{\mathbb{L}/\Bbbk}(X)$ be the corresponding field polynomials. Then

$$F_{\mathbb{L}/\Bbbk}(X) = \big(F_{\mathbb{K}/\Bbbk}(X)\big)^m.$$

Consequently $N_{\mathbb{L}/\Bbbk}(a) = (N_{\mathbb{K}/\Bbbk}(a))^m$ and $\mathrm{Tr}_{\mathbb{L}/\Bbbk}(a) = m\,\mathrm{Tr}_{\mathbb{K}/\Bbbk}(a)$.

PROOF. Proposition 9.54 shows that the matrix of $XI - M_{\mathbb{L}/\Bbbk}(a)$ may be taken to be block diagonal with each of the m diagonal blocks equal to the matrix of $XI - M_{\mathbb{K}/\Bbbk}(a)$. The determinant of $XI - M_{\mathbb{L}/\Bbbk}(a)$ is the product of the determinants of the diagonal blocks, and the formula relating the field polynomials is proved.

The formulas for the norms and the traces are consequences of this relationship. In fact, let

$$F_{\mathbb{K}/\Bbbk}(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0$$

and

$$F_{\mathbb{L}/\Bbbk}(X) = X^{mn} + d_{mn-1}X^{mn-1} + \cdots + d_0.$$

Comparing coefficients of $F_{\mathbb{L}/\Bbbk}(X)$ and $\big(F_{\mathbb{K}/\Bbbk}(X)\big)^m$, we see that $d_{mn-1} = mc_{n-1}$ and $d_0 = c_0^m$. Therefore

$$N_{\mathbb{L}/\Bbbk}(a) = (-1)^{mn}d_0 = ((-1)^n c_0)^m = (N_{\mathbb{K}/\Bbbk}(a))^m$$

and

$$\mathrm{Tr}_{\mathbb{L}/\Bbbk}(a) = -d_{mn-1} = -mc_{n-1} = m\,\mathrm{Tr}_{\mathbb{K}/\Bbbk}(a).$$

This completes the proof. □

Corollary 9.56. Let $\mathbb{K}/\Bbbk$ be a finite extension of fields, and let a be in $\mathbb{K}$. Then the field polynomial of a relative to $\mathbb{K}/\Bbbk$ is a power of the minimal polynomial of a over $\Bbbk$, the power being $[\mathbb{K} : \Bbbk(a)]$. In the special case $\mathbb{K} = \Bbbk(a)$, the minimal polynomial of a coincides with the field polynomial.

REMARKS. In the theory of a single linear transformation as in Chapter V, the minimal polynomial of a linear map divides the characteristic polynomial, by the Cayley–Hamilton Theorem (Theorem 5.9). For a multiplication operator in the context of fields, we get a much more precise result—that the characteristic polynomial is a power of the minimal polynomial.

PROOF. If $F(X)$ is in $\Bbbk[X]$, then the operation M of multiplication has

$$M(F(a))b = F(a)b = F(M(a))b \qquad \text{for } b \in \mathbb{K}, \tag{$*$}$$

as we see by first considering monomials and then forming $\Bbbk$ linear combinations. The minimal polynomial of a over $\Bbbk$ is the unique monic $F(X)$ of lowest degree in $\Bbbk[X]$ for which $F(a) = 0$, hence such that $M(F(a)) = 0$. Meanwhile, the minimal polynomial of the linear map $M(a)$ is the unique monic $F(X)$ of lowest degree such that $F(M(a)) = 0$. These two polynomials coincide because of $(*)$.

The degree of the minimal polynomial of $M(a)$ thus equals the degree of the minimal polynomial of a, which is $[\Bbbk(a) : \Bbbk]$. The Cayley–Hamilton Theorem (Theorem 5.9) shows that the minimal polynomial of $M(a)$ divides the characteristic polynomial of $M(a)$, i.e., the field polynomial of a. When the field $\mathbb{K}$ is $\Bbbk(a)$, the minimal polynomial of a and the field polynomial of a have the same

Pure Mathematical Physics

degree; since they are monic, they are equal. This proves the second conclusion of the corollary.

For the first conclusion we know from Corollary 9.55 that the field polynomial of a relative to a general $\mathbb{K}$ is the $[\mathbb{K} : \Bbbk(a)]^{\text{th}}$ power of the field polynomial of a relative to $\Bbbk(a)$. Since we have just seen that the latter polynomial is the minimal polynomial of a, the first conclusion of the corollary follows. □

EXAMPLE, CONTINUED. $\Bbbk = \mathbb{Q}$, $\mathbb{K} = \mathbb{Q}(\sqrt{2}\,)$, $a = \sqrt{2}$. We have seen that the field polynomial of a is $X^2 - 2$, that the norm and trace are $N(a) = -2$ and $\mathrm{Tr}(a) = 0$, and that the matrix of the multiplication operator $M(a)$ in the ordered basis $\Gamma = (1, \sqrt{2}\,)$ is $\begin{pmatrix} M(a) \\ \Gamma\Gamma \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$. The eigenvalues of $\begin{pmatrix} M(a) \\ \Gamma\Gamma \end{pmatrix}$ are $\pm\sqrt{2}$, namely the roots of the field polynomial. These are not in the field $\Bbbk$. Indeed, they could not possibly be in the field, or we would have $M(a)x = \lambda x$ for some $x \neq 0$ in $\mathbb{K}$ and some λ in $\Bbbk$, and this would mean that $\lambda = a$. Since the roots $\pm\sqrt{2}$ of the field polynomial each have multiplicity 1 and lie in $\mathbb{K}$, the matrix $\begin{pmatrix} M(a) \\ \Gamma\Gamma \end{pmatrix}$ is similar over $\mathbb{K}$ to the diagonal matrix $\begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}$. Since similar matrices have the same trace and the same norm, we can compute the trace and norm of $M(a)$ from this diagonal matrix, namely by adding or multiplying its diagonal entries. The significance of the diagonal entries is that they are the images of $\sqrt{2}$ under the members of the Galois group $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. We shall now generalize these considerations. Additional complications arise when $\mathbb{K}/\Bbbk$ fails to be separable and normal.[18]

Proposition 9.57. Let $\Bbbk$ be a field, let $\Bbbk(a)$ be an algebraic extension of $\Bbbk$, and suppose that the minimal polynomial $F(X)$ of a over $\Bbbk$ is separable. Let $\mathbb{K}$ be a splitting field of $F(X)$, and factor $F(X)$ over $\mathbb{K}$ as

$$F(X) = (X - a_1)(X - a_2) \cdots (X - a_n)$$

with all $a_j \in \mathbb{K}$ and with $a_1 = a$. Then the matrix of the multiplication operator $M(a)_{\Bbbk(a)/\Bbbk}$ of a on $\Bbbk(a)$ is similar over $\mathbb{K}$ to a diagonal matrix with diagonal entries $a_1, \ldots, a_n$. Consequently

$$N_{\Bbbk(a)/\Bbbk}(a) = \prod_{j=1}^{n} a_j \qquad \text{and} \qquad \mathrm{Tr}_{\Bbbk(a)/\Bbbk}(a) = \sum_{j=1}^{n} a_j.$$

[18]The above argument used a matrix with entries in $\Bbbk$ and considered the entries as in the larger field $\mathbb{K}$. The reader may wonder what the corresponding construction is for the $\Bbbk$ linear map $M(a)$. It is *not* to treat $M(a)$ as a $\mathbb{K}$ linear map on $\mathbb{K}$, since then $M(a)$ would have just the one eigenvalue $\sqrt{2}$, which would have multiplicity 1. Instead, it is to use tensor products as in Chapter VI, knowledge of which is not being assumed at present. The idea is to extend scalars, replacing $\mathbb{K}$ by $\mathbb{K} \otimes_{\Bbbk} \mathbb{K}$ and replacing $M(a)$ by $M(a) \otimes 1$. The $\mathbb{K}$ linearity occurs in the second member of the tensor product, not the first, and the operator $M(a) \otimes 1$ is the $\mathbb{K}$ linear map with eigenvalues $\pm\sqrt{2}$.

REMARKS. The elements $a_1, \dots, a_n$ of $\mathbb{K}$, with $a_1 = a$, are called the **conjugates** of a over $\Bbbk$. The conjugates of a are the images of a under the Galois group when $\Bbbk(a)$ is Galois over $\Bbbk$, but they extend outside $\Bbbk$ when $\Bbbk(a)/\Bbbk$ is not normal.

PROOF. Corollary 9.56 shows that $F(X)$ equals the field polynomial of a relative to $\Bbbk(a)/\Bbbk$, i.e., is the characteristic polynomial of the multiplication operator $M_{\Bbbk(a)/\Bbbk}(a)$. Let A be the matrix of $M_{\Bbbk(a)/\Bbbk}(a)$ in some ordered basis of $\Bbbk(a)$ over $\Bbbk$. If we regard A as a matrix with entries in $\mathbb{K}$, then the characteristic polynomial of A splits in $\mathbb{K}$, and the roots of the characteristic polynomial have multiplicity 1, by separability. Consequently A has a basis of eigenvectors, the eigenvectors being column vectors with entries in $\mathbb{K}$ and the eigenvalues being the members $a_1, \dots, a_n$ of $\mathbb{K}$. It follows that A is similar over $\mathbb{K}$ to a diagonal matrix with diagonal entries $a_1, \dots, a_n$. The determinant and trace of this diagonal matrix equal the determinant and trace of A, and therefore the norm and trace of a are the product and sum of the members $a_1, \dots, a_n$ of $\mathbb{K}$. □

Corollary 9.58. Let $\mathbb{K}$ be a finite Galois extension of the field $\Bbbk$, let $G = \mathrm{Gal}(\mathbb{K}/\Bbbk)$, let $\mathbb{L}$ be an intermediate field with $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$, and let $H = \mathrm{Gal}(\mathbb{K}/\mathbb{L})$ as a subgroup of G. Fix an ordered basis Γ of $\mathbb{L}$ over $\Bbbk$. Then the expression "$\sigma(a)$ for $\sigma \in G/H$" is well defined for a in $\mathbb{L}$, and there exists a nonsingular matrix C of size $[\mathbb{L} : \Bbbk]$ with entries in $\mathbb{K}$ such that every a in $\mathbb{L}$ has $C^{-1}\begin{pmatrix} M_{\mathbb{L}/\Bbbk}(a) \\ & \ddots \\ & & M_{\mathbb{L}/\Bbbk}(a) \end{pmatrix} C$ diagonal with diagonal entries $\sigma(a)$ for $\sigma \in G/H$. In particular, every member a of $\mathbb{L}$ has norm and trace given by

$$N_{\mathbb{L}/\Bbbk}(a) = \prod_{\sigma \in G/H} \sigma(a) \qquad \text{and} \qquad \mathrm{Tr}_{\mathbb{L}/\Bbbk}(a) = \sum_{\sigma \in G/H} \sigma(a).$$

PROOF. Let a be in $\mathbb{L}$, σ be in G, and τ be in H. Then $\tau(a) = a$, and therefore $\sigma\tau(a) = \sigma(a)$. Consequently all members of the coset σH of G/H have the same value on a, and "$\sigma(a)$ for $\sigma \in G/H$" is well defined.

Let $n = [\mathbb{L} : \Bbbk] = |G/H|$. Fix an ordered basis Γ of $\mathbb{L}$ over $\Bbbk$. For each $a \in \mathbb{L}$, let $A(a)$ be the matrix of the multiplication operator $M(a)_{\mathbb{L}/\Bbbk}$ relative to Γ.

The Theorem of the Primitive Element (Theorem 9.34) shows that $\mathbb{L} = \Bbbk(x)$ for some x. Proposition 9.57 applies to this element x and to a splitting field within $\mathbb{K}$ for its minimal polynomial, showing that there is a nonsingular matrix C with entries in $\mathbb{K}$ such that $C^{-1}A(x)C$ is a diagonal matrix whose diagonal entries are the n conjugates $x_1, \dots, x_n$ of x in $\mathbb{K}$, x_1 being x; the diagonal entries are necessarily distinct by separability. For each i with $1 \le i \le n$, there exists σ_i in G with $\sigma_i(x) = x_i$ by Theorems 9.11 and 9.23. Since H fixes $\mathbb{L}$, every member of the coset $\sigma_i H$ carries x to x_i. On the other hand, every σ in G must carry x to some conjugate, hence must have $\sigma(x) = \sigma_i(x)$ for some i. Then $\sigma_i^{-1}\sigma$ fixes x

Pure Mathematical Physics

and hence $\mathbb{L}$, and it follows that $\sigma_i^{-1}\sigma$ is in H. Thus σ is in $\sigma_i H$. In other words, the conjugates $x_1, \ldots, x_n$ may be regarded exactly as the images of the n cosets $\sigma_j H$.

In this terminology the diagonal entries of $C^{-1}A(x)C$ are the n elements $\sigma(x)$ for σ in G/H. For each j with $0 \le j \le n-1$, we have $A(x^j) = A(x)^j$, and hence $C^{-1}A(x^j)C = C^{-1}A(x)^j C$ is diagonal with diagonal entries $\sigma(x)^j = \sigma(x^j)$ for σ in G/H. Forming $\Bbbk$ linear combinations, we see for every polynomial $P(X)$ in $\Bbbk[X]$ of degree $\le n-1$ that $C^{-1}A(P(x))C$ is diagonal with diagonal entries $\sigma(P(x))$. Every element a of $\mathbb{K}$ is of the form $P(x)$ for some such $P(X)$, and the existence of C in the statement of the corollary is proved. The formulas for the norm and trace follow by taking the determinant and trace. □

Corollary 9.59. If $\mathbb{K}$ is a finite separable extension of the field $\Bbbk$, then the trace function $\mathrm{Tr}_{\mathbb{K}/\Bbbk}$ is not identically 0.

REMARKS. This result is trivial in characteristic 0 because $\mathrm{Tr}_{\mathbb{K}/\Bbbk}(1) = [\mathbb{K} : \Bbbk]$ is not zero. The result is not so evident in characteristic p, and the assumption of separability is crucial. An example for which separability fails and the trace function is identically 0 has $\Bbbk = \mathbb{F}(x)$, where $\mathbb{F}$ is a finite field of characteristic p and x is transcendental, and $\mathbb{K} = \Bbbk(x^{1/p})$. The basis elements $1, x^{1/p}, x^{2/p}, \ldots, x^{(p-1)/p}$ all have trace 0, and therefore the trace is identically 0.

PROOF. By the Theorem of the Primitive Element (Theorem 9.34), we can write $\mathbb{K} = \Bbbk(a)$ for some $a \neq 0$. Let $\mathbb{K}'$ be a splitting field for the minimal polynomial of a over $\Bbbk$. Then $\mathbb{K}'/\Bbbk$ is a separable extension by Corollary 9.30 and hence is a finite Galois extension. Proposition 9.57 shows that the matrix of $M_{\mathbb{K}/\Bbbk}(a)$ in any ordered basis of $\mathbb{K}$ over $\Bbbk$ is similar over $\mathbb{K}'$ to a diagonal matrix with entries $a_1, \ldots, a_n$, where $a_1, \ldots, a_n$ are the conjugates of a with $a_1 = a$. These conjugates are necessarily distinct by separability. For $1 \le k \le n$, the matrix of $M_{\mathbb{K}/\Bbbk}(a^k)$ is similar via the same matrix over $\mathbb{K}'$ to a diagonal matrix with entries $a_1^k, \ldots, a_n^k$. If $\mathrm{Tr}_{\mathbb{K}/\Bbbk}(a^k) = 0$ for $1 \le k \le n$, then we obtain the homogeneous system of linear equations

$$\begin{aligned} a_1x_1 + a_2x_2 + \cdots + a_nx_n &= 0, \\ a_1^2x_1 + a_2^2x_2 + \cdots + a_n^2x_n &= 0, \\ &\vdots \\ a_1^nx_1 + a_2^nx_2 + \cdots + a_n^nx_n &= 0, \end{aligned}$$

with $(x_1, \ldots, x_n) = (1, \ldots, 1)$ as a nonzero solution. The coefficient matrix must therefore have determinant 0. This coefficient matrix, however, is a Vandermonde matrix except that the j^{th} column is multiplied by a_j for each j. Since $a_1, \ldots, a_n$

Pure Mathematical Physics

are distinct, Corollary 5.3 shows that the determinant of the coefficient matrix can be 0 only if $a_1 a_2 \cdots a_n = 0$. Since $a \neq 0$, we have arrived at a contradiction, and we conclude that $\mathrm{Tr}_{\mathbb{K}/\Bbbk}(a^k) \neq 0$ for some k. □

With the aid of Corollary 9.59, we can complete the proof of Theorem 8.54 in Section VIII.11. Let us restate the part that still needs proof.

THEOREM 8.54. If R is a Dedekind domain with field of fractions F and if K is a finite separable extension field of F, then the integral closure T of R in K is finitely generated as an R module and consequently is a Dedekind domain.

REMARKS. What needs proof is that T is finitely generated as an R module. It was shown in Section VIII.11 how to deduce as a consequence that T is a Dedekind domain.

PROOF. Since R is Noetherian (being a Dedekind domain), Proposition 8.34 shows that it is enough to exhibit T as an R submodule of a finitely generated R module in K. Let $\{u_1, \ldots, u_n\}$ be a vector-space basis of K over F. Proposition 8.42 shows that we may assume that each u_i is in T.

Define an F linear map from K into its F vector-space dual K' by $y \mapsto \ell_y$, where $\ell_y(x) = \mathrm{Tr}_{K/F}(xy)$ for $x \in K$. This map is one-one by Corollary 9.59, and the equality of dimensions of K and K' over F therefore implies that the map is onto. We can thus view every member of K' as uniquely of the form ℓ_y for some y in K. With this understanding, let $\{\ell_{v_1}, \ldots, \ell_{v_n}\}$ be the dual basis of K' with $\ell_{v_j}(u_i) = \delta_{ij}$ for all i and j. Then we have

$$\mathrm{Tr}_{K/F}(u_i v_j) = \delta_{ij} \qquad \text{for all } i \text{ and } j.$$

Applying Proposition 8.42, choose $c \neq 0$ in R with cv_j in T for all j. We shall complete the proof by showing that

$$T \subseteq Rc^{-1}u_1 + \cdots + Rc^{-1}u_n. \tag{$*$}$$

Before doing so, let us observe that

$$\mathrm{Tr}_{K/F}(t) \quad \text{is in } R \text{ if } t \text{ is in } T. \tag{$**$}$$

In fact, Proposition 9.57 shows that $\mathrm{Tr}_{F(t)/F}(t)$ is the sum of all the conjugates of t, whether or not they are in K. The conjugates have the same minimal polynomial over F that t has, and hence they are integral over R. Their sum $\mathrm{Tr}_{F(t)/F}(t)$ must be integral over R by Corollary 8.38, and it must lie in F. Since R is integrally closed (being a Dedekind domain), $\mathrm{Tr}_{F(t)/F}(t)$ lies in R. This proves $(**)$.

Now we can return to the proof of $(*)$. Let x be given in T. Since T is a ring, cxv_j is in T for each j, and $\mathrm{Tr}_{K/F}(cxv_j)$ is in R by $(**)$. Since $\{u_1, \ldots, u_n\}$ is a

Pure Mathematical Physics

basis, we can write $x = \sum_i d_i u_i$ with each d_i in F. Since $\mathrm{Tr}(cxv_j)$ is in R, the computation

$$\mathrm{Tr}(cxv_j) = c\,\mathrm{Tr}_{K/F}(xv_j) = c\sum_{i=1}^{n} d_i\,\mathrm{Tr}(u_i v_j) = cd_j$$

shows that cd_j is in R. Then the expansion $x = \sum_i (cd_i)c^{-1}u_i$ exhibits x as in $Rc^{-1}u_1 + \cdots + Rc^{-1}u_n$ and completes the proof of $(*)$. □

16. Splitting of Prime Ideals in Extensions

Section VIII.7 was a section of motivation showing the importance for number theory and geometry of passing from factorization of elements to factorization of ideals. The later sections of Chapter VIII set the framework for this study, examining the notions of Noetherian domain, integral closure, and localization and putting them together in the notion of Dedekind domain. Only just now were we able to complete the proof of the fundamental result (Theorem 8.54) for constructing Dedekind domains out of other Dedekind domains. However, that proposition does not complete the task of extending what is in Section VIII.7 to a wider context. Much of Section VIII.7 concerned the relationship between prime ideals in one domain and prime ideals in an extension. In the present section we put that relationship in a wider context, showing how the examples of Section VIII.7 are special cases of the present theory.

In two of the examples in Section VIII.7, we worked with the ring $\mathbb{Z}$ of integers inside its field of fractions $\mathbb{Q}$ and with the ring T of algebraic integers within a quadratic extension $\mathbb{K}$ of $\mathbb{Q}$. In the third example in that section, we worked with the ring $\mathbb{C}[x]$, for transcendental x, inside its field of fractions $\mathbb{C}(x)$ and with a certain integral domain T within a quadratic extension of $\mathbb{C}(x)$. For all three examples we saw a correspondence between prime ideals P in T and prime ideals (p) in $\mathbb{Z}$ or $\mathbb{C}[x]$, and that correspondence was formalized in a more general setting in Propositions 8.43 and 8.53. The objective now is to understand that correspondence a little better.

The notation for this section is as follows: Let R be a Dedekind domain, such as $\mathbb{Z}$ or $\mathbb{C}[x]$, and let F be its field of fractions.[19] Let K be a finite separable extension of F, and let T be the integral closure of R in K. Theorem 8.54, including the part just proved in the previous section, shows that T is a Dedekind domain. We make repeated use of the fact about Dedekind domains that every nonzero prime ideal is maximal.

[19] It might seem more natural to assume that R is a principal ideal domain, as it is with $\mathbb{Z}$ and $\mathbb{C}[x]$. But that extra assumption will not help us, and it will often not be satisfied when the present results are used in the proof of the important Theorem 9.64 in the next section.

Pure Mathematical Physics

Proposition 8.43 shows that if P is any nonzero prime ideal of T, then $\mathfrak{p} = R \cap P$ is a nonzero prime ideal of R. In the reverse direction Proposition 8.53 shows that if $\mathfrak{p}$ is any nonzero prime ideal in R, then $\mathfrak{p}T \neq T$, and there exists at least one prime ideal P of T with $\mathfrak{p} = R \cap P$. The unique factorization of ideals in T (given as Theorem 8.55) explains this correspondence better. If $\mathfrak{p}$ is given, then $\mathfrak{p}T$ is a proper ideal, hence is contained in some maximal ideal P. Since "to contain is to divide" (by Theorem 8.55d), such P's (and only such P's) are factors in the decomposition of $\mathfrak{p}T$ as the product of nonzero prime ideals. Accordingly let us write

$$\mathfrak{p}T = \prod_{i=1}^{g} P_i^{e_i},$$

where the P_i are the distinct prime ideals of T containing $\mathfrak{p}T$, or equivalently the distinct prime ideals of T satisfying $R \cap P_i = \mathfrak{p}$. The e_i are positive integers called the **ramification indices**.

For each P_i, we can form the composition $R \subseteq T \to T/P_i$ of inclusion followed by passage to the quotient. Since $\mathfrak{p} \subseteq P_i$, this composition descends to a ring homomorphism $R/\mathfrak{p} \to T/P_i$. The ideal $\mathfrak{p}$ is maximal in R, and the ideal P_i is maximal in T. Thus the mapping $R/\mathfrak{p} \to T/P_i$ is in fact a field map. We regard it as an inclusion. Define

$$f_i = [T/P_i : R/\mathfrak{p}],$$

allowing the dimension for the moment possibly to be $+\infty$. It will follow from Theorem 9.60, however, that f_i is finite. The integer f_i is called the **residue class degree**.

Theorem 9.60. Let R be a Dedekind domain, let F be its field of fractions, let K be a finite separable extension of F with $[K : F] = n$, and let T be the integral closure of R in K. If $\mathfrak{p}$ is a nonzero prime ideal in R and $\mathfrak{p}T = \prod_{i=1}^{g} P_i^{e_i}$ is a decomposition of $\mathfrak{p}T$ as the product of powers of distinct nonzero prime ideals in T, then the ramification indices e_i and residue class degrees $f_i = [T/P_i : R/\mathfrak{p}]$ are related by

$$\sum_{i=1}^{g} e_i f_i = n.$$

REMARKS. Consequently each f_i is finite. The cases of interest for our earlier examples have $R = \mathbb{Z}$ or $R = \mathbb{C}[x]$. When $R = \mathbb{Z}$, each $R/\mathfrak{p}$ is a finite field. However, when $R = \mathbb{K}[x]$ for some field $\mathbb{K}$ of characteristic 0 like $\mathbb{K} = \mathbb{C}$, then each $R/\mathfrak{p}$ is a finite extension of $\mathbb{K}$, hence is an infinite field.[20]

[20] When $R = \mathbb{C}[x]$, then $T/P_i = R/\mathfrak{p} \cong \mathbb{C}$ since $\mathbb{C}$ is algebraically closed. The last example of the present section will elaborate.

PROOF. Corollary 8.63 gives a ring isomorphism

$$T/(\mathfrak{p}T) \cong T/P_1^{e_1} \times \cdots \times T/P_g^{e_g}. \tag{$*$}$$

Recall from the definition of residue class degree that we have a field mapping of $R/\mathfrak{p}$ into each T/P_i. Since $\mathfrak{p} \subseteq P_i^e$ for $1 \le e \le e_i$ and since $\mathfrak{p} \subseteq \mathfrak{p}T$, it follows similarly that we have a one-one ring homomorphism of $R/\mathfrak{p}$ into each T/P_i^e with $1 \le e \le e_i$ and another one-one ring homomorphism of $R/\mathfrak{p}$ into $T/(\mathfrak{p}T)$. Consequently each T/P_i^e with $1 \le e \le e_i$, the product $T/P_1^{e_1} \times \cdots \times T/P_g^{e_g}$, and $T/(\mathfrak{p}T)$ may all be regarded as unital $R/\mathfrak{p}$ modules, i.e., as vector spaces over the field $R/\mathfrak{p}$. Fix i. For $1 \le e \le e_i$, let us prove by induction on e that

$$\dim_{R/\mathfrak{p}}(T/P_i^e) = ef_i, \tag{$**$}$$

the case $e = 1$ being the base case of the induction. Assume inductively that $(**)$ holds for exponents from 1 to $e-1$. We know from Corollary 8.60 that P_i^{e-1}/P_i^e is a vector space over the field T/P_i with

$$\dim_{T/P_i}(P_i^{e-1}/P_i^e) = 1. \tag{$\dagger$}$$

The First Isomorphism Theorem (as in the remark with Theorem 8.3) gives $T/P_i^{e-1} \cong (T/P_i^e)\big/(P_i^{e-1}/P_i^e)$ as vector spaces over $R/\mathfrak{p}$, and it follows that

$$\begin{aligned}\dim_{R/\mathfrak{p}}(T/P_i^e) &= \dim_{R/\mathfrak{p}}(T/P_i^{e-1}) + \dim_{R/\mathfrak{p}}(P_i^{e-1}/P_i^e)\\ &= (e-1)f_i + f_i = ef_i,\end{aligned}$$

the next-to-last equality following from $(\dagger)$ and the inductive hypothesis for the cases $e-1$ and 1. This completes the induction and the proof of $(**)$.

In view of the decomposition $(*)$ and the formula $(**)$ when $e = e_i$, the theorem will follow if it is shown that

$$\dim_{R/\mathfrak{p}}(T/(\mathfrak{p}T)) = n. \tag{$\dagger\dagger$}$$

To prove $(\dagger\dagger)$ we localize. Let S be the complement of the prime ideal $\mathfrak{p}$ of R. Corollary 8.48 shows that $S^{-1}R$ is a Dedekind domain, Corollary 8.50 shows that $S^{-1}\mathfrak{p}$ is its unique maximal ideal, and Corollary 8.62 shows that $S^{-1}R$ is a principal ideal domain.

The composition $R \subseteq S^{-1}R \to S^{-1}R/S^{-1}\mathfrak{p}$ descends to a field mapping $R/\mathfrak{p} \to S^{-1}R/S^{-1}\mathfrak{p}$. Let us see that this mapping is onto. If $s_0^{-1}r_0 + S^{-1}\mathfrak{p}$ in $S^{-1}R/S^{-1}\mathfrak{p}$ is given, then s_0 is not in $\mathfrak{p}$, and the maximality of $\mathfrak{p}$ as an ideal in R implies that $(s_0) + \mathfrak{p} = R$. Therefore we can choose r in R and x in $\mathfrak{p}$ with $rs_0 + x = r_0$. Under the mapping $R/\mathfrak{p} \to S^{-1}R/S^{-1}\mathfrak{p}$, the image of $r + \mathfrak{p}$ is

Pure Mathematical Physics

$r + S^{-1}\mathfrak{p} = r + s_0^{-1}x + S^{-1}\mathfrak{p} = s_0^{-1}(rs_0 + x) + S^{-1}\mathfrak{p} = s_0^{-1}r_0 + S^{-1}\mathfrak{p}$. Thus our mapping is onto $S^{-1}R/S^{-1}\mathfrak{p}$, and we have an isomorphism of fields

$$R/\mathfrak{p} \cong S^{-1}R/S^{-1}\mathfrak{p}. \tag{‡}$$

Similarly the composition $T \subseteq S^{-1}T \to S^{-1}T/(S^{-1}\mathfrak{p}T)$ descends to a homomorphism of rings $T/\mathfrak{p}T \to S^{-1}T/(S^{-1}\mathfrak{p}T)$. Let us show that this map too is one-one onto.

If $t + \mathfrak{p}T$ is in the kernel, then the member t of T is in $S^{-1}\mathfrak{p}T$, and st is in $\mathfrak{p}T$ for some s in S. Hence we have $(s)(t) \subseteq P_1^{e_1} \cdots P_g^{e_g}$, and we can write $(s)(t) = P_1^{e_1} \cdots P_g^{e_g} Q$ for some ideal Q. Factoring the principal ideals (s) and (t) and using the uniqueness of factorization of ideals gives

$$(s) = P_1^{u_1} \cdots P_g^{u_g} Q_1 \qquad \text{and} \qquad (t) = P_1^{v_1} \cdots P_g^{v_g} Q_2$$

with $Q = Q_1 Q_2$ and with $u_j + v_j = e_j$ for all j. If $u_j > 0$, then we must have $(s) \subseteq P_j$ and $sR \subseteq P_j \cap R = \mathfrak{p}$. This says that s is in $\mathfrak{p}$, in contradiction to the fact that S equals the set-theoretic complement of $\mathfrak{p}$ in R. We conclude that $u_j = 0$ for all j. Therefore $(t) = P_1^{e_1} \cdots P_g^{e_g} Q_2 \subseteq P_1^{e_1} \cdots P_g^{e_g} = \mathfrak{p}T$, and t is in $\mathfrak{p}T$. Consequently the kernel consists of the 0 coset alone.

Let us show that $T/\mathfrak{p}T$ maps onto $S^{-1}T/(S^{-1}\mathfrak{p}T)$. If $s_0^{-1}t_0 + S^{-1}\mathfrak{p}T$ in $S^{-1}T/S^{-1}\mathfrak{p}T$ is given, then s_0 is not in $\mathfrak{p}$, and the maximality of $\mathfrak{p}$ as an ideal in R implies that $(s_0) + \mathfrak{p} = R$. Therefore we can choose r in R and x in $\mathfrak{p}$ with $rs_0 + x = 1$, hence with $rs_0t_0 + xt_0 = t_0$. Under the mapping $T/\mathfrak{p}T \to S^{-1}T/(S^{-1}\mathfrak{p}T)$, the image of $rt_0 + \mathfrak{p}T$ is

$$\begin{aligned} rt_0 + S^{-1}\mathfrak{p}T &= rt_0 + s_0^{-1}xt_0 + S^{-1}\mathfrak{p}T \\ &= s_0^{-1}(rs_0t_0 + xt_0) + S^{-1}\mathfrak{p}T \\ &= s_0^{-1}t_0 + S^{-1}\mathfrak{p}T. \end{aligned}$$

Thus our mapping is onto $S^{-1}T/S^{-1}\mathfrak{p}T$, and we conclude that we have an isomorphism of rings

$$T/\mathfrak{p}T \to S^{-1}T/(S^{-1}\mathfrak{p}T). \tag{‡‡}$$

Since T is finitely generated as an R module (Theorem 8.54), $S^{-1}T$ is finitely generated as an $S^{-1}R$ module with the same generators. Since $S^{-1}R$ is a principal ideal domain, Theorem 8.25c shows that $S^{-1}T$ is the direct sum of cyclic $S^{-1}R$ modules. Each of these cyclic modules must in fact be isomorphic to $S^{-1}R$ since $S^{-1}T$ has no zero divisors, and therefore $S^{-1}T$ is a free $S^{-1}R$ module of some finite rank m. If $t_1, \ldots, t_m$ are free generators, then we have

$$S^{-1}T = S^{-1}Rt_1 + \cdots + S^{-1}Rt_m. \tag{§}$$

Pure Mathematical Physics

Let us see that $\{t_1, \dots, t_m\}$ is an F vector-space basis of K. Suppose $\sum_j c_j t_j = 0$ with all c_j in F. Proposition 8.42 shows that there is an $r \neq 0$ in R with $rc_1, \dots, rc_m$ in R. Then $\sum_j (rc_j)t_j = 0$, and the independence of $t_1, \dots, t_m$ over $S^{-1}R$ implies that $rc_j = 0$ for all j. Thus $c_j = 0$ for all j, and we obtain linear independence over F. If $x \in K$ is given, we can choose $r \neq 0$ in R with rx in T by Proposition 8.42. Since $t_1, \dots, t_m$ span $S^{-1}T$ over $S^{-1}R$, we can find members $d_1, \dots, d_m$ of $S^{-1}R$ with $rx = \sum_j d_j t_j$. Then $x = \sum_j r^{-1} d_j t_j$ with each coefficient $r^{-1}d_j$ in F. This proves the spanning. Hence $\{t_1, \dots, t_m\}$ is an F vector-space basis, and $m = n$.

To complete the proof of (††) and hence the theorem, it is enough, in view of the isomorphisms (‡) and (‡‡), to prove that the cosets $t_j + S^{-1}\mathfrak{p}T$ in $S^{-1}T/(S^{-1}\mathfrak{p}T)$ form a vector-space basis over $S^{-1}R/S^{-1}\mathfrak{p}$. If t is in $S^{-1}T$, then (§) says that $t = \sum c_j t_j$ with c_j in $S^{-1}R$. Hence

$$t + S^{-1}\mathfrak{p}T = \sum (c_j + S^{-1}\mathfrak{p})(t_j + S^{-1}\mathfrak{p}T),$$

and we have spanning. If $\sum_j (c_j + S^{-1}\mathfrak{p})(t_j + S^{-1}\mathfrak{p}T) = 0 + S^{-1}\mathfrak{p}T$, then $\sum_j c_j t_j$ is in $S^{-1}\mathfrak{p}T$. Thus we can write $\sum_j c_j t_j = \sum_i a_i t_i'$ with $a_i \in \mathfrak{p}$ and $t_i' \in S^{-1}T$. Expanding each t_i' according to (§), substituting, and using the uniqueness of the expansion (§), we see for each j that c_j is a sum of products of the a_i's by members of $S^{-1}R$. Therefore each c_j is in $S^{-1}\mathfrak{p}$. This proves the linear independence and establishes (††). □

The case of greatest interest is that K is a finite Galois extension of F. In this case the statement of Theorem 9.60 simplifies and will be given in its simplified form as Theorem 9.62. We begin with a lemma.

Lemma 9.61. Let R be a Dedekind domain, let F be its field of fractions, let K be a finite separable extension of F, and let T be the integral closure of R in K. Suppose that K is Galois over F. If $\mathfrak{p}$ is a nonzero prime ideal in R and $\mathfrak{p}T = \prod_{i=1}^{g} P_i^{e_i}$ is a decomposition of $\mathfrak{p}T$ as the product of nonzero prime ideals in T, then $\mathrm{Gal}(K/F)$ is transitive on the set of ideals $\{P_1, \dots, P_g\}$.

PROOF. Arguing by contradiction, suppose that P_j is not of the form $\sigma(P_1)$ for some σ in $\mathrm{Gal}(K/F)$. By the Chinese Remainder Theorem we can choose an element t of T with $t \equiv 0 \bmod P_j$ and $t \equiv 1 \bmod \sigma(P_1)$ for all σ. Every σ in $\mathrm{Gal}(K/F)$ carries t to a member of T since t and $\sigma(t)$ have the same minimal polynomial over F. Corollary 9.58 shows that $N_{K/F}(t) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(t)$, and consequently $N_{K/F}(t)$ is in $T \cap F = R$. Since the factor t itself is in P_j, $N_{K/F}(t)$ is in P_j. Therefore $N_{K/F}(t)$ is in $R \cap P_j = \mathfrak{p} \subseteq \prod_{i=1}^{g} P_i^{e_i}$. The right side is contained in P_1. Since P_1 is prime, some factor $\sigma_l(t)$ of $N_{K/F}(t)$ is in P_1. Then t is in $\sigma_l^{-1}(P_1)$, in contradiction to the fact that $t \equiv 1 \bmod \sigma(P_1)$ for all σ. □

Pure Mathematical Physics

Theorem 9.62. Let R be a Dedekind domain, let F be its field of fractions, let K be a finite separable extension of F with $[K : F] = n$, and let T be the integral closure of R in K. Suppose that K is Galois over F. If $\mathfrak{p}$ is a nonzero prime ideal in R and $\mathfrak{p}T = \prod_{i=1}^{g} P_i^{e_i}$ is a decomposition of $\mathfrak{p}T$ as the product of powers of distinct nonzero prime ideals in T, then the ramification indices have $e_1 = \cdots = e_g$, and the residue class degrees $f_i = [T/P_i : R/\mathfrak{p}]$ have $f_1 = \cdots = f_g$. If e and f denote the common value of the e_i's and of the f_j's, then

$$\boxed{efg = n\,.}$$

PROOF. For σ in $\mathrm{Gal}(K/F)$, apply σ to the factorization $\mathfrak{p}T = \prod_{i=1}^{g} P_i^{e_i}$, obtaining

$$\mathfrak{p}T = \sigma(P_1)^{e_1} \prod_{i=2}^{g} \sigma(P_i)^{e_i}.$$

Lemma 9.61 shows that $\sigma(P_1)$ can be any P_j, and unique factorization of ideals (Theorem 8.55) therefore implies that $e_1 = e_j$. With the same σ, the fact that σ respects the field operations implies that

$$T/P_1 \cong \sigma(T)/\sigma(P_1) = T/P_j,$$

and thus $f_1 = f_j$. Substituting the values of the e_i's and the f_j's into the formula of Theorem 9.60, we obtain $efg = n$. □

EXAMPLES WITH $n = 2$ CONTINUED FROM SECTION VIII.7.

(1) $R = \mathbb{Z}$ and $T = \mathbb{Z}[\sqrt{-1}\,]$. In this case, $\mathbb{Z}$ and T are both principal ideal domains. We found three possible behaviors[21] for the prime factorization of a principal ideal $(p)T$ in T generated by a prime $p > 0$ in $\mathbb{Z}$:

(a) $(p)T$ is prime in T if $p = 4m + 3$. Here $e = g = 1$; so $f = 2$.
(b) $(p)T = (a + ib)(a - ib)$ with $p = a^2 + b^2$ if $p = 4m + 1$. Here $e = 1$ and $g = 2$; so $f = 1$.
(c) $(2)T = (1 + i)^2$. Here $e = 2$ and $g = 1$; so $f = 1$.

(2) $R = \mathbb{Z}$ and $T = \mathbb{Z}[\sqrt{-5}\,]$. In this case, T is not a unique factorization domain and is in particular not a principal ideal domain. We gave examples of three possible behaviors for the prime factorization of a principal ideal $(p)T$ in T generated by a prime $p > 0$ in $\mathbb{Z}$:

(a) $(11)T$ is prime in T. Here $e = g = 1$; so $f = 2$.
(b) $(2)T = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$. Here $e = 1$ and $g = 2$; so $f = 1$.
(c) $(5)T = (\sqrt{-5}\,)^2$. Here $e = 2$ and $g = 1$; so $f = 1$.

[21] The notation here fits with the notation in Theorem 9.62 and is different from the notation in Section VIII.7.

Pure Mathematical Physics

(3) $R = \mathbb{C}[x]$ and $T = \mathbb{C}[x, \sqrt{(x-1)x(x+1)}\,]$. In this case, R is a principal ideal domain, and we saw that T is not a unique factorization domain. We found two possible behaviors for the prime factorization of a principal ideal $(p)T$ in T generated by a prime p in $\mathbb{C}[x]$:

(a) $(x - x_0)T = (x - x_0, y - y_0)(x - x_0, y + y_0)$ if the equal expressions $y_0^2 = (x_0 - 1)x_0(x_0 + 1)$ are not 0. Here $e = 1$ and $g = 2$; so $f = 1$.

(b) $(x - x_0)T = (x - x_0, y)^2$ if x_0 is in $\{-1, 0, +1\}$. Here $e = 2$ and $g = 1$; so $f = 1$.

The third type, with $(x - x_0)T$ prime in T, does not arise. It cannot arise since $f > 1$ would point to a quadratic extension of $\mathbb{C}$, yet $\mathbb{C}$ is algebraically closed.

17. Two Tools for Computing Galois Groups

In Section 8 we mentioned that the effect of the Fundamental Theorem of Galois Theory is to reduce the extremely difficult problem of finding intermediate fields to the less-difficult problem of finding a Galois group. In the intervening sections we have seen some illustrations of the power of this reduction, all in cases in which the Galois group was close at hand.

The problem of finding a Galois group in a particular situation is usually not as easy as in those cases, and it by no means can be considered as solved in general. In this section we combine Galois theory with some of the ring theory in the second half of Chapter VIII in order to develop two tools that sometimes help identify particular Galois groups.

Let us think in terms of a finite Galois extension K of the rationals $\mathbb{Q}$. The field K is the splitting field of some irreducible monic polynomial with rational coefficients, and we can scale this polynomial's indeterminate (in effect by multiplying its roots by some nonzero integer) so that the polynomial is monic and has integer coefficients. Thus let $F(X)$ be a monic irreducible polynomial in $\mathbb{Z}[X]$ of some degree d, and let K be its splitting field over $\mathbb{Q}$. The members of $\mathrm{Gal}(K/\mathbb{Q})$ are determined by their effect on the d roots of $F(X)$, and hence $\mathrm{Gal}(K/\mathbb{Q})$ may be regarded as a subgroup of the symmetric group $\mathfrak{S}_d$. If $r_1, \ldots, r_d$ are the roots of $F(X)$, then the **discriminant** of $F(X)$ is the member of K defined by

$$D = \prod_{1 \le i < j \le d} (r_j - r_i)^2.$$

This was defined in Section 13 in the cases $d = 2$ and $d = 3$, and we computed the value of D in those cases. The discriminant is an integer under our hypotheses, and it is computable even though the roots $r_1, \ldots, r_d$ of $F(X)$ are not at hand. In fact, the proof of Theorem 9.50 indicates that the discriminant D is given by the determinant

$$D = \det \begin{pmatrix} d & a_1 & a_2 & \cdots & a_{d-1} \\ a_1 & a_2 & a_3 & \cdots & a_d \\ a_2 & a_3 & a_4 & \cdots & a_{d+1} \\ & & & \vdots & \\ a_{d-1} & a_d & a_{d+1} & \cdots & a_{2d-2} \end{pmatrix},$$

where $a_j = r_1^j + r_2^j + \cdots + r_d^j$. Problems 36–39 at the end of Chapter VIII show that each of $a_1, \ldots, a_{2d-1}$ can be expressed as a polynomial in the elementary symmetric polynomials in $r_1, \ldots, r_d$, i.e., in the coefficients of $F(X)$, and doing so in a symbolic manipulation program is manageable for any fixed degree.[22]

The first of the two tools that sometimes help in identifying particular Galois groups directly concerns the discriminant: the discriminant is a square if and only if the Galois group is a subgroup of the alternating group. Let us state the result in the context of a general finite Galois extension even though we shall use it only for our Galois extension $K/\mathbb{Q}$.

Proposition 9.63. Let $\mathbb{K}/\Bbbk$ be a finite Galois extension, and suppose that $\mathbb{K}$ is the splitting field of a separable polynomial $F(X)$ in $\Bbbk[X]$ of degree d. Let D be the discriminant of $F(X)$, and regard $G = \mathrm{Gal}(\mathbb{K}/\Bbbk)$ as a subgroup of the symmetric group $\mathfrak{S}_d$. Then D is in $\Bbbk$, and G is a subgroup of the alternating group $\mathfrak{A}_d$ if and only if D is the square of an element of $\Bbbk$.

REMARK. The proof will use Galois theory to show that D is in $\Bbbk$, and Problems 36–39 at the end of Chapter VIII do not need to be invoked.

PROOF. Let $r_1, \ldots, r_d$ be the roots of $F(X)$, and put $\Delta = \prod_{i<j}(r_j - r_i)$. Under the identification of G with a subgroup of the permutation group $\mathfrak{S}_d$ on $\{1, \ldots, d\}$, each σ in G has

$$\sigma(\Delta) = \prod_{i<j} (\sigma(r_j) - \sigma(r_i)) = \prod_{i<j} (r_{\sigma(j)} - r_{\sigma(i)}) = (\operatorname{sgn}\sigma) \prod_{i<j} (r_j - r_i) = (\operatorname{sgn}\sigma)\Delta.$$

[22] For example, when $d = 3$, let $F(X) = X^3 - c_1X^2 + c_2X - c_3$. In Mathematica the following program produces a_1, a_2, a_3, a_4 as output:

```
e1={a1==r1+r2+r3, r1+r2+r3==c1, r1 r2+r2 r3+r1 r3==c2,
    r1 r2 r3==c3}
Eliminate[e1,{r1,r2,r3}]
e2={a2==r1^2+r2^2+r3^2, r1+r2+r3==c1, r1 r2+r2 r3+r1 r3==c2,
    r1 r2 r3==c3}
Eliminate[e2,{r1,r2,r3}]
e3={a3==r1^3+r2^3+r3^3, r1+r2+r3==c1, r1 r2+r2 r3+r1 r3==c2,
    r1 r2 r3==c3}
Eliminate[e3,{r1,r2,r3}]
e4={a4==r1^4+r2^4+r3^4, r1+r2+r3==c1, r1 r2+r2 r3+r1 r3==c2,
    r1 r2 r3==c3}
Eliminate[e4,{r1,r2,r3}]
```


Pure Mathematical Physics

In particular, the element $D = \Delta^2$ has $\sigma(D) = D$. By Proposition 9.35d, D is in $\mathbb{k}$.

If some σ in G has $\operatorname{sgn}\sigma = -1$, then σ does not fix Δ, and Δ is not in $\mathbb{k}$. Since Δ is a square root of D and since any two square roots of an element in a field differ at most by a sign, D is not the square of any element of $\mathbb{k}$.

Conversely if every σ in G has $\operatorname{sgn}\sigma = +1$, then every σ fixes Δ, and Proposition 9.35d shows that Δ is in $\mathbb{k}$. Since $D = \Delta^2$, D is the square of the member Δ of $\mathbb{k}$. □

The second tool is complicated to prove but simple to state. We reduce the polynomial $F(X)$ modulo p for each prime number p and form the associated finite splitting field. The Galois group for a finite extension of finite fields is cyclic by Proposition 9.40, and we thus obtain a cyclic subgroup of $\mathfrak{S}_d$. The second tool is this: if p does not divide the discriminant of $F(X)$, then this cyclic group as a permutation group is a subgroup of $\operatorname{Gal}(K/\mathbb{Q})$ as a permutation group, up to a relabeling of the symbols. In other words, the order *and cycle structure* of a generator of the cyclic group are the same as the order and cycle structure of some element of $\operatorname{Gal}(K/\mathbb{Q})$.

Let us formulate the result precisely. In the setting of Theorem 9.62, fix a prime ideal P of T lying in the factorization of $\mathfrak{p}T$. Each member σ of $G = \operatorname{Gal}(K/F)$ carries T to itself, but not every σ in G carries P to itself. Let G_P be the isotropy subgroup of G at P, i.e., let $G_P = \{\sigma \in G \mid \sigma(P) = P\}$. The subgroup G_P is called the **decomposition group** at P. Each σ in G_P descends to an automorphism of the field T/P that fixes the subfield $R/\mathfrak{p}$, since σ fixes each element of R. Thus σ defines a member $\overline{\sigma}$ of $\overline{G} = \operatorname{Gal}((T/P)/(R/\mathfrak{p}))$ by the formula

$$\overline{\sigma}(\bar{x}) = \overline{\sigma(x)}, \qquad \text{where } \bar{y} = y + P \text{ for } y \in T.$$

It is apparent that $\sigma \mapsto \overline{\sigma}$ is a homomorphism of G into $\overline{G}$. This homomorphism turns out to yield the result stated informally in the previous paragraph. It has the key property given in Theorem 9.64.

Theorem 9.64. Let R be a Dedekind domain, let F be its field of fractions, let K be a finite separable extension of F with $[K : F] = n$, and let T be the integral closure of R in K. Suppose that K is Galois over F. Let $\mathfrak{p}$ be a nonzero prime ideal in R, let $P = P_1$ be a prime factor in a decomposition $\mathfrak{p}T = \prod_{i=1}^{g} P_i^{e_i}$ of $\mathfrak{p}T$ as the product of powers of distinct nonzero prime ideals in T, and suppose that T/P is a Galois extension of $R/\mathfrak{p}$. Let $G = \operatorname{Gal}(K/F)$, $G_P = \{\sigma \in G \mid \sigma(P) = P\}$, and $\overline{G} = \operatorname{Gal}((T/P)/(R/\mathfrak{p}))$. Then the group homomorphism $\sigma \mapsto \overline{\sigma}$ of G_P into $\overline{G}$ carries G_P onto $\overline{G}$.

Pure Mathematical Physics

REMARKS. In our application with $R = \mathbb{Z}$, T/P and $R/\mathfrak{p}$ are finite fields, and Proposition 9.40 shows that T/P is a Galois extension of $R/\mathfrak{p}$ with no further assumptions.

PROOF. Let K^d be the fixed field of G_P within K; Theorem 9.38 shows that $\mathrm{Gal}(K/K^d) = G_P$. Let T^d be the integral closure of R in K^d; this is a Dedekind domain, and T is the integral closure of T^d in K. We are going to apply Theorem 9.62 with R in the theorem replaced[23] by T^d.

Proposition 8.43 shows that $\mathcal{P} = T^d \cap P$ is a nonzero prime ideal of T^d. Since every member of G_P carries P to itself and since G_P is the full Galois group of K over K^d, Lemma 9.61 shows that P is the only nonzero prime ideal of T whose intersection with T^d is $\mathcal{P}$. Therefore $\mathcal{P}T^d = P^{e'}$ for some integer $e' \geq 1$.

As always, we have a field mapping $R/\mathfrak{p} \to T^d/\mathcal{P}$. Let us show that this mapping is onto $T^d/\mathcal{P}$. For any given u in T^d, we are to produce r in R with

$$r \equiv u \bmod \mathcal{P}. \tag{$*$}$$

Each σ in G that is not in G_P has $\sigma^{-1}P \neq P$, and the previous paragraph shows that the nonzero prime ideal $\mathcal{P}_\sigma = T^d \cap \sigma^{-1}P$ of T^d has $\mathcal{P}_\sigma \neq T^d \cap P$. Therefore $\mathcal{P}_\sigma + \mathcal{P} = T^d$, and the Chinese Remainder Theorem (Theorem 8.27) shows that we can find an element v of T^d with

$$v \equiv u \bmod \mathcal{P} \qquad \text{and} \qquad v \equiv 1 \bmod \mathcal{P}_\sigma$$

for all σ that lie in G but not G_P. The first congruence implies that $v - u$ is in $\mathcal{P} = T^d \cap P \subseteq P$, hence that

$$v \equiv u \bmod P, \tag{$**$}$$

while the second congruence implies that $v - 1$ is in $\mathcal{P}_\sigma = T^d \cap \sigma^{-1}P \subseteq \sigma^{-1}P$, hence that $\sigma(v-1)$ lies in P. Therefore

$$\sigma(v) \equiv 1 \bmod P \qquad \text{for all } \sigma \text{ in } G \text{ but not } G_P. \tag{$\dagger$}$$

Put $r = N_{K^d/F}(v)$. Since the splitting field of the minimal polynomial of v over F is contained in K, Corollary 9.58 shows that r is the product of the elements $\sigma(v)$ for σ in G/G_P. Each of these is in T, and hence $N_{K^d/F}(v)$ is in T. Since $N_{K^d/F}(v)$ is also in F, $r = N_{K^d/F}(v)$ is in $T \cap F = R$. If we use $\sigma = 1$ as the representative of the identity coset of G/G_P, then we have

$$r = N_{K^d/F}(v) = v\Big(\prod_{\substack{\text{some } \sigma\text{'s} \\ \text{not in } G_P}} \sigma(v)\Big).$$

[23] Consequently it would not have been sufficient to prove Theorem 9.62 when the ring R is a principal ideal domain.

Pure Mathematical Physics

The factor of v is congruent to u mod P by $(**)$, and each factor in parentheses is congruent to 1 mod P by $(\dagger)$. Therefore $r \equiv u \bmod P$, and $r - u$ is in P. Since $r - u$ is in T^d, $r - u$ is in $T^d \cap P = \mathcal{P}$. This proves $(*)$. Consequently we can identify $\overline{G} = \mathrm{Gal}((T/P)/(R/\mathfrak{p}))$ with $\mathrm{Gal}((T/P)/(T^d/\mathcal{P}))$.

Choose $\bar{x}_1$ in T/P with $T/P = (T^d/\mathcal{P})[\bar{x}_1]$; this choice is possible by the assumed separability of $(T/P)/(R/\mathfrak{p})$. Let x_1 be a member of T with $\bar{x}_1 = x_1 + P$, and let $M(X)$ be the minimal polynomial of x_1 over K^d. Since x_1 is in T, the coefficients of $M(X)$ are in T^d. Let $\overline{M}(X)$ be the corresponding member of $(T^d/\mathcal{P})[X]$, given by the substitution homomorphism that takes T^d to $T^d/\mathcal{P}$ and takes X to X. Since K/K^d is normal, $M(X)$ splits over K. Write $x_1, \dots, x_n$ for its roots; these are in T.

Let τ be given in $\overline{G}$, and suppose that $\tau(\bar{x}_1) = \bar{x}_j$. Since $M(X)$ is irreducible over K^d, the Galois group $\mathrm{Gal}(K/K^d) = G_P$ is transitive on its roots. Choose σ in G_P with $\sigma(x_1) = x_j$. Then $\overline{\sigma}(\bar{x}_1) = \bar{x}_j$. Since $\overline{\sigma}$ and τ agree on the generator $\bar{x}_1$ of T/P over $T^d/\mathcal{P}$, they agree on T/P. Therefore τ is exhibited as the image of σ under the homomorphism of the theorem, and the proof is complete. □

A first consequence of Theorem 9.64 is that we get interpretations of the integers e, f, and g, and they will be helpful to us. Galois theory gives us $|G| = n$, and Theorem 9.62 says that $efg = n$. The transitivity in Lemma 9.61 says that G acts transitively on the set $\{P_1, \dots, P_g\}$, and the isotropy subgroup at $P = P_1$ is G_P. Hence $g|G_P| = |G|$, and $|G_P| = n/g = ef$. Galois theory gives us $|\overline{G}| = f$, and the fact that G_P maps onto $\overline{G}$ says that $G_P/\mathrm{kernel} \cong \overline{G}$; therefore $|\mathrm{kernel}| = |G_P|/|\overline{G}| = (ef)/f = e$. We conclude that g is the number of cosets modulo G_P, e is the order of the kernel of the homomorphism in Theorem 9.64, and f is the order of the cyclic group $\overline{G}$.

In the setting of interest for current purposes, we are taking $R = \mathbb{Z}$, $F = \mathbb{Q}$, and K equal to the splitting field of a given monic irreducible polynomial $F(X)$ of degree d in $\mathbb{Z}[X]$. We will be using Theorem 9.64 for various choices of $\mathfrak{p} = (p)$ in $\mathbb{Z}$ to make progress on identifying $\mathrm{Gal}(K/\mathbb{Q})$. In order to identify $\overline{G}$ with the subgroup G_P of G, we need the kernel of the homomorphism of G_P onto $\overline{G}$ to be trivial. From the previous paragraph we know that the condition in question is that $e = 1$. We postpone to Chapter V of *Advanced Algebra* any justification of the assertion that $e = 1$ if p does not divide the discriminant of $F(X)$.

In previous sections we have identified $\mathrm{Gal}(K/\mathbb{Q})$ in some cases when the Galois group is relatively small compared with the degree d of the polynomial. The method now is helpful when the Galois group is relatively large compared with d.

Let us be sure when $e = 1$ that the theorem is telling us not only that G_P is isomorphic to $\overline{G}$ as an abstract group, but also that the cycle structure of the elements of $\overline{G}$ is the same as the cycle structure of the elements of G_P. For this

purpose we ignore the proof of the theorem and concentrate only on the statement. Assuming that p does not divide the discriminant, let $\overline{F}(X)$ be the reduction of $F(X)$ modulo p, let $r_1, \dots, r_d$ be the roots of $F(X)$ in T, and let $\bar{r}_1, \dots, \bar{r}_d$ be the images of $r_1, \dots, r_d$ under the quotient homomorphism $T \to T/P$. The elements $\bar{r}_1, \dots, \bar{r}_d$ are distinct since p does not divide the discriminant of $F(X)$. Any member σ of $G = \mathrm{Gal}(K/\mathbb{Q})$ permutes $r_1, \dots, r_d$ and is determined by the resulting permutation since K is assumed to be generated by $r_1, \dots, r_d$. Under the assumption that σ is in G_P, σ descends to an automorphism $\overline{\sigma}$ of T/P. This automorphism $\overline{\sigma}$ acts on the set of elements $\bar{r}_1, \dots, \bar{r}_d$, permuting them. Since the mapping of the r_j's to the $\bar{r}_j$'s is one-one, the resulting permutation of the subscripts $1, \dots, d$ is the same.

When p varies, we cannot match the elements $\bar{r}_1, \dots, \bar{r}_d$ for one value of p with those for another value of p, because we have no direct knowledge of $r_1, \dots, r_d$. Thus we cannot directly compare the permutation groups $\overline{G}$ that we obtain for different p's. But at least we know their cycle structure.

To apply the theory, we factor $\overline{F}(X)$ quickly with a symbolic manipulation program, and we obtain the Galois group of a splitting field of $\overline{F}(X)$ by inspection, together with the cycle structure of its elements. Specifically an irreducible factor of degree m contributes an m-cycle for the element, and the cycles corresponding to distinct irreducible factors are disjoint. Then we put together the information from various p's and see what elements must be in $\mathrm{Gal}(K/\mathbb{Q})$, up to a relabeling of indices.

EXAMPLE 1. $F(X) = X^5 - X - 1$. The discriminant is $D = 2869 = 19 \cdot 151$. Thus the method may be used with any prime number other than 19 and 151. Here is the factorization for a few primes, together with the cycle structure within $\mathfrak{S}_5$ for a generator of $\overline{G}$:

p	$\overline{F}(X)$	Cycle lengths
2	$(X^2 + X + 1)(X^3 + X + 1)$	2, 3
3	$X^5 + 2X + 2$	5
17	$(X + 9)(X + 11)(X^3 + 14X^2 + 12X + 6)$	1, 1, 3
23	$(X + 9)(X^4 + 14X^3 + 12X^2 + 7X + 5)$	1, 4

For comparison, $p = 19$ gives $\overline{F}(X) = (X + 6)^2(X^2 + 7X^2 + 13X + 10)$, but we cannot use this prime since it divides the discriminant. It is enough to use the information from $p = 2$ and $p = 3$. The irreducibility modulo 3 implies irreducibility over $\mathbb{Q}$. From $p = 3$, we obtain a 5-cycle in $\mathrm{Gal}(K/\mathbb{Q})$. From $p = 2$, we obtain the product of a 2-cycle and a 3-cycle, and the cube of this element is a 2-cycle. In the example in Section 11 following the statement of Theorem 9.44, we saw in effect that the only subgroup of $\mathfrak{S}_5$ containing a 5-cycle and a 2-cycle is $\mathfrak{S}_5$ itself. Therefore $\mathrm{Gal}(K/\mathbb{Q}) = \mathfrak{S}_5$.

Pure Mathematical Physics

EXAMPLE 2. $F(X) = X^5 + 10X^3 - 10X^2 + 35X - 18$. The discriminant is $D = 3025000000 = 2^6 5^8 11^2$, a perfect square. Thus the Galois group is a subgroup of the alternating group $\mathfrak{A}_5$. The method using reduction modulo p may be used with any prime other than 2, 5, and 11. Here is the factorization for a few primes, together with the cycle structure within $\mathfrak{S}_5$ for a generator of $\overline{G}$:

p	$\overline{F}(X)$	Cycle lengths
3	$X(X+2)(X^3+X^2+2X+1)$	1, 1, 3
7	$X^5+3X^3+4X^2+3$	5
17	$(X+14)(X^2+5X+14)(X^2+15X+15)$	1, 2, 2

It is enough to use the information from $p = 3$ and $p = 7$. The irreducibility modulo 7 implies irreducibility over $\mathbb{Q}$. From $p = 7$, we obtain a 5-cycle in $\mathrm{Gal}(K/\mathbb{Q})$. From $p = 3$, we obtain a 3-cycle. Any 5-cycle and any 3-cycle together generate all of $\mathfrak{A}_5$. In fact, the generated subgroup must have order divisible by 15, hence must have order 15, 30, or 60. It cannot be of order 15 because every group of order 15 is cyclic and $\mathfrak{A}_5$ has no elements of order 15. It cannot be of order 30 because $\mathfrak{A}_5$ is simple and subgroups of index 2 have to be normal. Hence it is all of $\mathfrak{A}_5$.

EXAMPLE 3. Galois group $\mathfrak{S}_d$. Given $d \geq 4$, let us see how to form an irreducible $F(X)$ for which $\mathrm{Gal}(K/\mathbb{Q})$ is all of $\mathfrak{S}_d$. For any degree d and any prime number ℓ, there exists at least one irreducible monic polynomial of degree d in $\mathbb{F}_\ell[X]$; the reason is that the finite field $\mathbb{F}_{\ell^d}$ is a simple extension of $\mathbb{F}_\ell$ by Corollary 9.19. Let $H_{d,2}(X)$ be such a polynomial of degree d for $\ell = 2$, and let $H_{d-1,3}(X)$ be such a polynomial of degree $d-1$ for $\ell = 3$. Then let p be a prime greater than d, and let $H_{2,p}(X)$ be an irreducible monic polynomial of degree 2 in $\mathbb{F}_p[X]$. We can regard each of $H_{d,2}(X)$, $H_{d-1,3}(X)$, and $H_{2,p}(X)$ as in $\mathbb{Z}[X]$ by reinterpreting their coefficients as integers. Consider the congruences

$$\begin{aligned} F[X] &\equiv H_{d,2}(X) && \mod (2), \\ F[X] &\equiv X H_{d-1,3}(X) && \mod (3), \\ F[X] &\equiv \Big(\prod_{k=0}^{d-3} (X-k)\Big) H_{2,p}(X) && \mod (p), \end{aligned}$$

in $\mathbb{Z}[X]$. Since the sum of any two of the three ideals (2), (3), and (p) of $\mathbb{Z}[X]$ is $\mathbb{Z}[X]$, the Chinese Remainder Theorem (Theorem 8.27) implies that there exists a simultaneous solution $F[X]$ to these congruences in $\mathbb{Z}[X]$, and we may take $F[X]$ to be monic of degree d. Let K be a splitting field for $F[X]$ over $\mathbb{Q}$. Our method applies to the primes 2, 3, and p since none of the three polynomials has any

repeated factors. The result of applying the method is that $\mathrm{Gal}(K/\mathbb{Q})$ contains a d-cycle, a $(d-1)$-cycle, and a 2-cycle. Let us see that the subgroup generated by these three elements is all of $\mathfrak{S}_d$. We may assume that the $(d-1)$-cycle is $(1\ 2\ \cdots\ d-1)$. Without loss of generality, the 2-cycle is either $(1\ \ j)$ with $j < d$ or is $(k\ \ d)$ with $k < d$. In the first case some power of the d-cycle is a permutation τ with $\tau(1) = d$; if σ denotes the 2-cycle $(1\ \ j)$, then Lemma 4.41 shows that $\tau\sigma\tau^{-1}$ is the 2-cycle $(d\ \ \tau(j))$, and this is of the form $(k\ \ d)$ with $k < d$. Thus we may assume in any event that $\mathrm{Gal}(K/\mathbb{Q})$ contains $(1\ \ 2\ \ \cdots\ \ d-1)$ and some 2-cycle $(k\ \ d)$ with $k < d$. Conjugating $(k\ \ d)$ by powers of $(1\ \ 2\ \ \cdots\ \ d-1)$, we see that $\mathrm{Gal}(K/\mathbb{Q})$ contains *every* 2-cycle $(k\ \ d)$ with $k < d$. For $1 \le k < d-1$, we then find that $\mathrm{Gal}(K/\mathbb{Q})$ contains

$$(k\ \ d)(k+1\ \ d)(k\ \ d) = (k\ \ k+1).$$

So $\mathrm{Gal}(K/\mathbb{Q})$ contains $(1\ \ 2)$, $(2\ \ 3)$, $\ldots$, $(d-2\ \ d-1)$, and we have already seen that it contains $(d-1\ \ d)$. These $d-1$ transpositions generate the full symmetric group, and therefore $\mathrm{Gal}(K/\mathbb{Q}) = \mathfrak{S}_d$.

18. Problems

1. Take as known that the polynomial $X^3 - 3X + 4$ is irreducible over $\mathbb{Q}$, and let r be a complex root of it. In the field $\mathbb{Q}(r)$, find a multiplicative inverse for $r^2 + r + 1$ and express it in the form $ar^2 + br + c$ with a, b, c in $\mathbb{Q}$.
2. Suppose that R is an integral domain and that F is a subring that is a field, so that R can be considered as a vector space over F. Prove that if $\dim_F R$ is finite, then R is a field.
3. Let $\mathbb{K}$ be a subfield of $\mathbb{C}$ that is not a subfield of $\mathbb{R}$. Prove that $\mathbb{K}$ is topologically dense in $\mathbb{C}$.
4. Let $\mathbb{K} = \Bbbk(x)$ be a transcendental extension of the field $\Bbbk$, and let y be a member of $\mathbb{K}$ that is not in $\Bbbk$. Prove that $\Bbbk(x)$ is an algebraic extension of $\Bbbk(y)$.
5. What is a necessary and sufficient condition on an integer $N > 0$ for the positive square root of N to be in the subfield $\mathbb{Q}(\sqrt[3]{2}\,)$ of $\mathbb{R}$?
6. The polynomials $F(X) = X^3 + X + 1$ and $G(Y) = Y^3 + Y^2 + 1$ are irreducible over $\mathbb{F}_2$. Let $\mathbb{K}$ be the field $\mathbb{K} = \mathbb{F}_2[X]/(F(X))$, and let $\mathbb{L}$ be the field $\mathbb{L} = \mathbb{F}_2[Y]/(G(Y))$. Since $\mathbb{K}$ and $\mathbb{L}$ are two fields of order 8, they must be isomorphic. Find an explicit isomorphism.
7. Can a field of order 8 have a subfield of order 4? Why or why not?
8. If $\mathbb{K}$ is a finite field, prove that the product of the nonzero elements of $\mathbb{K}$ is -1. (Educational note: When $\mathbb{K}$ is $\mathbb{F}_p$, this result reduces to Wilson's Theorem, given as Problem 8 at the end of Chapter IV.)
9. Suppose that $\mathbb{K}/\Bbbk$ is a finite extension of the form $\mathbb{K} = \Bbbk(r)$ with $[\mathbb{K} : \Bbbk]$ odd. Prove that $\mathbb{K} = \Bbbk(r^2)$.

Pure Mathematical Physics

10. Suppose that $\mathbb{K}/\Bbbk$ is a finite extension of fields and that $\mathbb{K} = \Bbbk[r, s]$. Prove that if $[\Bbbk(r) : \Bbbk]$ is relatively prime to $[\Bbbk(s), \Bbbk]$, then
    (a) the minimal polynomial of r over $\Bbbk$ is irreducible over $\Bbbk(s)$,
    (b) $[\mathbb{K} : \Bbbk] = [\Bbbk(r) : \Bbbk]\,[\Bbbk(s) : \Bbbk]$.

11. In $\mathbb{C}$, let $\beta = \sqrt[3]{2}$, $\omega = \frac{1}{2}(-1 + \sqrt{-3})$, and $\alpha = \omega\beta$.
    (a) Prove for all c in $\mathbb{Q}$ that $\gamma = \beta + c\alpha$ is a root of some sixth-degree polynomial of the form $X^6 + aX^3 + b$.
    (b) Prove that the minimal polynomial of $\beta + \alpha$ over $\mathbb{Q}$ has degree 3.
    (c) Prove that the minimal polynomial of $\beta - \alpha$ over $\mathbb{Q}$ has degree 6.

12. Suppose that $\Bbbk$ is a finite field and that $F(X)$ is a member of $\Bbbk[X]$ whose derivative is the 0 polynomial. Prove that $F(X)$ is reducible over $\Bbbk$.

13. Let $\Bbbk$ be a field, let $F(X)$ be a separable polynomial in $\Bbbk[X]$, let $\mathbb{K}$ be a splitting field of $F(X)$ over $\Bbbk$, and let $r_1, \dots, r_n$ be the roots of $F(X)$ in $\mathbb{K}$. Regard $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ as a subgroup of the symmetric group $\mathfrak{S}_n$.
    (a) Prove that $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is transitive on $\{r_1, \dots, r_n\}$ if and only if $F(X)$ is irreducible over $\Bbbk$.
    (b) Show that the cyclotomic polynomial $\Phi_8(X)$ is an example with $\Bbbk = \mathbb{Q}$ and $n = 4$ for which $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is transitive but $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ contains no 4-cycle.
    (c) Prove that if n is prime and $F(X)$ is irreducible over $\Bbbk$, then $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ contains an n-cycle.

14. Let $a_1, \dots, a_n$ be relatively prime square-free integers ≥ 2, and define $\mathbb{L}_k = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_k})$ for $0 \leq k \leq n$.
    (a) Show for each k that $[\mathbb{L}_k : \mathbb{Q}] = 2^l$ with $0 \leq l \leq k$.
    (b) Suppose for a particular k that $[\mathbb{L}_k : \mathbb{Q}] = 2^k$. Exhibit a vector-space basis of $\mathbb{L}_k$ over $\mathbb{Q}$, and describe the members of $\mathrm{Gal}(\mathbb{L}_k/\mathbb{Q})$ by telling the effect of each member on all basis vectors of $\mathbb{L}_k$ over $\mathbb{Q}$.
    (c) Suppose for a particular $k < n$ that $[\mathbb{L}_k : \mathbb{Q}] = 2^k$. Assume that $\sqrt{a_{k+1}}$ lies in $\mathbb{L}_k$, and let $\sqrt{a_{k+1}}$ be expanded in terms of the basis of (b). Show that application of the members of $\mathrm{Gal}(\mathbb{L}_k/\mathbb{Q})$ leads to a contradiction.
    (d) Deduce that $[\mathbb{L}_n : \mathbb{Q}] = 2^n$.

15. Let p be a prime number, and suppose that a is a member of $\mathbb{Q}$ such that $X^p - a$ has no root in $\mathbb{Q}$. If r is a member of $\mathbb{C}$ with $r^p = a$, prove that
    (a) the cyclotomic polynomial $\Phi_p(X)$ is irreducible in $\mathbb{Q}(r)$,
    (b) the splitting field $\mathbb{K}$ of $X^p - a$ over $\mathbb{Q}$ has degree $[\mathbb{K} : \mathbb{Q}] = p(p-1)$,
    (c) the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is isomorphic to a semidirect product of the multiplicative group of $\mathbb{F}_p$ and the additive group of $\mathbb{F}_p$, with the action of a member m of the multiplicative group on the members n of the additive group being given by $m(n) = mn$.

16. Let $F(X)$ be a polynomial in $\Bbbk[X]$ of degree n, where $\Bbbk$ is a field of characteristic 0, and let $\mathbb{K}$ be a splitting field for $F(X)$ over $\Bbbk$. Prove that $[\mathbb{K} : \Bbbk]$ divides $n!$.

17. Let $\Bbbk$ be a field, and let $\mathbb{K}$ be a quadratic extension $\Bbbk(r)$, where $r^2 = a$ is a member of $\Bbbk$.
    (a) If $\Bbbk$ has characteristic 0, determine all elements of $\mathbb{K}$ whose squares are in $\Bbbk$.
    (b) What happens differently if the characteristic is different from 0?

18. Let G be a finite group. Show that there exist two finite extensions $\Bbbk$ and $\mathbb{K}$ of $\mathbb{Q}$ such that $\mathbb{K}$ is a Galois extension of $\Bbbk$ and the Galois group $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is isomorphic to G.

19. Let $\mathbb{K}/\Bbbk$ be a finite normal extension. For $F(X)$ in $\mathbb{K}[X]$ and σ in $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, let $F^\sigma(X)$ be the result of the substitution homomorphism $\mathbb{K}[X] \to \mathbb{K}[X]$ carrying X to X and extending the action of σ on $\mathbb{K}$, i.e., let $F^\sigma(X)$ be obtained by applying σ to the coefficients of $F(X)$. Prove that $\prod_{\sigma \in \mathrm{Gal}(\mathbb{K}/\Bbbk)} F^\sigma(X)$ is in $\Bbbk[X]$.

20. Corollary 9.37 concerns a separable algebraic extension $\mathbb{K}/\Bbbk$ and a finite subgroup H of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, showing that $\mathbb{K}/\mathbb{K}^H$ is a finite Galois extension with $H = \mathrm{Gal}(\mathbb{K}/\mathbb{K}^H)$ and $[\mathbb{K} : \mathbb{K}^H] = |H|$. By going over its proof, obtain the conclusion that if $\{x_1, \ldots, x_n\}$ is the H orbit of x_1 in $\mathbb{K}$, then
    (a) the minimal polynomial of x_1 over $\mathbb{K}^H$ is $\prod_{j=1}^n (X - x_j)$.
    (b) n divides $|H|$.
    (c) $\mathbb{K} = \mathbb{K}^H(x_1)$ if the isotropy subgroup of H at x_1 is trivial.

21. Let $\mathbb{K}$ be the transcendental extension $\mathbb{C}(z)$ of $\mathbb{C}$.
    (a) Prove that any linear fractional transformation $\varphi(z) = \frac{az+b}{cz+d}$ with $ad-bc \neq 0$ in $\mathbb{C}$ extends uniquely to a $\mathbb{C}$ automorphism of $\mathbb{K}$.
    (b) Let H be the 4-element subgroup of $\mathrm{Gal}(\mathbb{K}/\mathbb{C})$ generated by the extensions of $\sigma(z) = -z$ and $\tau(z) = 1/z$. Show that $w = z^2 + z^{-2}$ is invariant under H, and conclude that every member of $\mathbb{C}(w)$ lies in $\mathbb{K}^H$.
    (c) Applying the previous problem to the element $x_1 = z$ of $\mathbb{K}$, show that the minimal polynomial of z over $\mathbb{C}(w)$ has degree 4.
    (d) Conclude that $\mathbb{K}^H = \mathbb{C}(z^2 + z^{-2})$.

22. In characteristic 0, let $\mathbb{L}/\mathbb{K}$ and $\mathbb{K}/\Bbbk$ be quadratic extensions.
    (a) Show that there exists an irreducible polynomial $F(X) = X^4 + bX^2 + c$ in $\Bbbk[X]$ such that $F(r) = 0$ for some r in $\mathbb{L}$.
    (b) Show that the element r in (a) has $\mathbb{L} = \Bbbk(r)$.
    (c) Show that $\mathbb{L}$ is a normal extension of $\Bbbk$ with Galois group $C_2 \times C_2$ if and only if c is a square in $\Bbbk$ for some polynomial as in (a), if and only if c is a square in $\Bbbk$ for every polynomial as in (a).

Pure Mathematical Physics

(d) Show that $\mathbb{L}$ is a normal extension of $\Bbbk$ with Galois group C_4 if and only if $c^{-1}(b^2 - 4c)$ is a square in $\Bbbk$ for some polynomial as in (a), if and only if $c^{-1}(b^2 - 4c)$ is a square in $\Bbbk$ for every polynomial as in (a).

(e) Give an example of quadratic extensions $\mathbb{L}/\mathbb{K}$ and $\mathbb{K}/\Bbbk$ in characteristic 0 such that $\mathbb{L}/\Bbbk$ is not normal.

23. Determine Galois groups for splitting fields over $\mathbb{Q}$ for the two polynomials $X^3 - 3X + 1$ and $X^3 + X + 1$.

24. Suppose that $F(X)$ is an irreducible cubic polynomial in $\mathbb{Q}[X]$ whose splitting field $\mathbb{K}$ has $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ isomorphic to $\mathfrak{S}_3$. What are the possibilities, up to isomorphism, for the Galois group of a splitting field of $(X^3 - 1)F(X)$ over $\mathbb{Q}$?

25. Let $\mathbb{K}/\Bbbk$ be a finite Galois extension whose Galois group is isomorphic to $\mathfrak{S}_3$. Is $\mathbb{K}$ necessarily a splitting field of some irreducible cubic polynomial in $\Bbbk[X]$? Why or why not?

26. Is Cardan's cubic formula valid for finding roots of reducible cubics $X^3 + pX + q$ in characteristic 0?

27. Prove that the discriminant of a real cubic with distinct roots is positive if all the roots are real, and is negative if two of the roots are complex.

28. Let $F(X) = X^3 + pX + q$ be irreducible in $\mathbb{Q}[X]$, and suppose that $X - r$ is a factor for some r in $\mathbb{C}$.

(a) Show that $F(X)$ factors in $\mathbb{Q}(r)[X]$ as $F(X) = (X - r)(X^2 + rX + (r^2 + p))$.

(b) We know that $\mathbb{Q}(r)$ is a splitting field for $F(X)$ over $\mathbb{Q}$ if and only if the discriminant $-4p^3 - 27q^2$ is a square in $\mathbb{Q}$. On the other hand, it is evident from the factorization of $F(X)$ that it splits is $\mathbb{Q}(r)$ if and only if the discriminant $r^2 - 4(r^2 + p)$ is a square in $\mathbb{Q}(r)$. Show by a direct calculation that these two conditions are equivalent.

29. Let $\mathbb{K}$ be a splitting field of an irreducible cubic polynomial $F(X)$ in $\mathbb{Q}[X]$. If $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is $\mathfrak{S}_3$, does it follow that $\mathbb{K}$ contains all three cube roots of 1? Why or why not?

30. In characteristic 0, let $\mathbb{K}$ be the splitting field over $\Bbbk$ of an irreducible polynomial in $\Bbbk[X]$ of degree 5. Assuming that the discriminant of the polynomial is a square in $\Bbbk$, what are the possibilities for $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ up to a relabeling of the indices?

31. Determine the Galois group of a splitting field over $\mathbb{Q}$ for the polynomial $X^5 + 6X^3 - 12X^2 + 5X - 4$. Use of a computer may be helpful for this problem.

32. The proof of Theorem 9.64 introduced a positive integer e' in its second paragraph. Prove that e' equals the integer e_1 in the statement of the theorem.

33. Let R be a Dedekind domain, let F be its field of fractions, let K be a finite separable extension of F, and let L be a finite separable extension of K. Let T be the integral closure of R in K, and let U be the integral closure of R in L. Let $\mathfrak{p}$, P, and Q be nonzero prime ideals in R, T, and U, respectively, and let the ramification indices and decomposition degrees for the extensions L/K, L/F, and K/F be

$$e(Q|P), e(P|\mathfrak{p}), e(Q|\mathfrak{p}) \qquad \text{and} \qquad f(Q|P), f(P|\mathfrak{p}), f(Q|\mathfrak{p}).$$

Prove that

$$e(Q|\mathfrak{p}) = e(Q|P)e(P|\mathfrak{p}) \qquad \text{and} \qquad f(Q|\mathfrak{p}) = f(Q|P)f(P|\mathfrak{p}).$$

Problems 34–40 concern norms and traces.

34. Let m be a square-free integer, and let N and Tr denote the norm and trace from $\mathbb{Q}(\sqrt{m}\,)$ to $\mathbb{Q}$.
    (a) Show that $N(a+b\sqrt{m}\,) = a^2 - mb^2$ and $\mathrm{Tr}(a+b\sqrt{m}\,) = 2a$.
    (b) Let T be the ring of algebraic integers in $\mathbb{Q}(\sqrt{m}\,)$. It was shown in Section VIII.9 that T consists of all $a+b\sqrt{m}$ with a, b in $\mathbb{Z}$ if $m \equiv 2 \bmod 4$ or $m \equiv 3 \bmod 4$, and of all $a+b\sqrt{m}$ with a, b in $\mathbb{Z}$ or a, b in $\mathbb{Z} + \frac{1}{2}$ if $m \equiv 1 \bmod 4$. Prove for $a+b\sqrt{m}$ in $\mathbb{Q}(\sqrt{m}\,)$ that $a+b\sqrt{m}$ is in T if and only if $N(a+b\sqrt{m}\,)$ and $\mathrm{Tr}(a+b\sqrt{m}\,)$ are both in $\mathbb{Z}$.
    (c) Assume that $a+b\sqrt{m}$ is in T. Prove that $N(a+b\sqrt{m}\,)$ is in $\mathbb{Z}^\times$ if and only if $a+b\sqrt{m}$ is in $T^\times$.
    (d) For $m = 2$, give an example of a member of $T^\times$ other than ± 1.

35. For the extension $\mathbb{Q}(\sqrt[3]{2}\,)/\mathbb{Q}$, find the value of the norm N and the trace Tr on a general element $a + b\sqrt[3]{2} + c(\sqrt[3]{2}\,)^2$ of $\mathbb{Q}(\sqrt[3]{2}\,)$; here a, b, c are in $\mathbb{Q}$.

36. Let $N(\,\cdot\,)$ be the norm relative to the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$, where ζ is a primitive n^{th} root of 1.
    (a) Show that $N(1-\zeta) = \Phi_n(1)$, where $\Phi_n(X)$ is the n^{th} cyclotomic polynomial.
    (b) Using the formula $\prod_{d|n,\ d>1} \Phi_d(X) = X^{n-1} + X^{n-2} + \cdots + 1$, show that $N(1-\zeta) = \Phi_n(1)$ equals p if n is a power of the positive prime p and equals 1 if n is divisible by more than one positive prime.

37. Let $p > 0$ be a prime in $\mathbb{Z}$ of the form $4n+1$. It was shown in Problem 31 at the end of Chapter VIII that such a prime is the sum of two squares. This problem gives a shorter proof. Take as known from Section VIII.4 that the ring $\mathbb{Z}[\sqrt{-1}\,]$ of Gaussian integers is a Euclidean domain, and from Problem 30 at the end of Chapter VIII that $x^2 \equiv -1 \bmod p$ has an integer solution x. Carry out the following steps:

Pure Mathematical Physics

(a) Write

$$\frac{x \pm \sqrt{-1}}{p} = \frac{1}{p}\, x \pm \frac{1}{p}\, \sqrt{-1}.$$

If p were prime in $\mathbb{Z}[\sqrt{-1}\,]$, then it would follow from the divisibility of $x^2 + 1$ by p that p divides $x + \sqrt{-1}$ or p divides $x - \sqrt{-1}$. Deduce from the displayed equation that neither alternative is viable, and conclude that p cannot be prime in $\mathbb{Z}[\sqrt{-1}\,]$.

(b) Using the conclusion of (a) to write p as a nontrivial product in $\mathbb{Z}[\sqrt{-1}]$ and applying the norm function, prove that there exist integers a and b such that $p = a^2 + b^2$.

38. Let $p > 0$ be a prime in $\mathbb{Z}$ of the form $8n + 1$. Take as known from Problem 13 at the end of Chapter VIII that $\mathbb{Z}[\sqrt{-2}\,]$ is a Euclidean domain, and from the law of quadratic reciprocity (to be proved in Chapter I of *Advanced Algebra*) that $x^2 \equiv -2 \bmod p$ has an integer solution x. Guided by the argument for the previous problem, prove that there exist integers a and b such that $p = a^2 + 2b^2$.

39. Let $p > 0$ be a prime in $\mathbb{Z}$ of the form $6n + 1$. Take as known from Problem 26 at the end of Chapter VIII that $\mathbb{Z}\big[\frac{1}{2}(1 + \sqrt{-3}\,)\big]$ is a Euclidean domain, and from the law of quadratic reciprocity (to be proved in *Advanced Algebra*) that $x^2 \equiv -3 \bmod p$ has an integer solution x. Guided by the argument for the previous problem, prove that there exist integers a and b such that $p = a^2 + 3b^2$.

40. Let $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{L}'$ be fields such that $\mathbb{L}'/\Bbbk$ is a finite separable extension. Using Corollary 9.58, prove that the norm and trace satisfy

$$N_{\mathbb{L}'/\Bbbk} = N_{\mathbb{L}/\Bbbk} \circ N_{\mathbb{L}'/\mathbb{L}} \qquad \text{and} \qquad \mathrm{Tr}_{\mathbb{L}'/\Bbbk} = \mathrm{Tr}_{\mathbb{L}/\Bbbk} \circ \mathrm{Tr}_{\mathbb{L}'/\mathbb{L}}\,.$$

Problems 41–45 make use of the theory of symmetric polynomials, which was introduced in Problems 36–39 at the end of Chapter VIII.

41. Let $\Bbbk$ be a field, let $F(X)$ be a polynomial in $\Bbbk[X]$, let $\mathbb{K}$ be an extension field in which $F(X)$ splits, and let $r_1, \ldots, r_n$ be the roots of $F(X)$ in $\mathbb{K}$, repeated according to their multiplicities. If $P(X_1, \ldots, X_n)$ is a symmetric polynomial in $\Bbbk[X_1, \ldots, X_n]$, prove that $P(r_1, \ldots, r_n)$ is a member of $\Bbbk$.

42. Let $\Bbbk$ be a field, let $F(X)$ and $G(X)$ be polynomials over $\Bbbk$, let $\mathbb{K}$ be an extension field in which $F(X)$ and $G(X)$ both split, and let $r_1, \ldots, r_m$ and $s_1, \ldots, s_n$ be the respective roots of $F(X)$ and $G(X)$ in $\mathbb{K}$, repeated according to their multiplicities. Deduce from the previous problem that the polynomials

$$H_1(X) = \prod_{i=1}^{m} \prod_{j=1}^{n} (X - r_i - s_j) \qquad \text{and} \qquad H_2(X) = \prod_{i=1}^{m} \prod_{j=1}^{n} (X - r_i s_j)$$

lie in $\Bbbk[X]$.

Pure Mathematical Physics

43. (a) Find a nonzero polynomial with rational coefficients having $\sqrt{2}+\sqrt{3}$ as a root. What is the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$?
    (b) Find a nonzero polynomial with rational coefficients having $\sqrt{2}+\sqrt[3]{2}$ as a root. What is the minimal polynomial of $\sqrt{2}+\sqrt[3]{2}$ over $\mathbb{Q}$?

44. Let $\Bbbk$ be a field of characteristic 0, and let $\mathbb{K} = \Bbbk(r_1, \ldots, r_n)$ be the field of fractions of the polynomial ring $\Bbbk[r_1, \ldots, r_n]$ in n indeterminates. Show that any σ in the symmetric group $\mathfrak{S}_n$ defines a member of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ such that $\sigma(r_j) = r_{\sigma(j)}$ for all σ in $\mathfrak{S}_n$. Then define $F(X)$ to be the polynomial

$$F(X) = (X - r_1)\cdots(X - r_n)$$

in $\mathbb{K}[X]$, and show that
    (a) $F(X)$ is irreducible over the fixed field $\mathbb{K}^{\mathfrak{S}_n}$,
    (b) $\mathbb{K}$ is a splitting field for $F(X)$ over $\mathbb{K}^{\mathfrak{S}_n}$,
    (c) $\mathbb{K}^{\mathfrak{S}_n} = \Bbbk(u_1, \ldots, u_n)$, where $u_1, \ldots, u_n$ are given by

$$u_1 = \sum_i r_I, \qquad u_2 = \sum_{i<j} r_i r_j, \qquad \ldots, \qquad u_n = \prod_i r_i,$$

    (d) the Galois group of the splitting field of $F(X)$ over $\Bbbk(u_1, \ldots, u_n)$ is $\mathfrak{S}_n$.

45. **(Cubic resolvent)** This problem carries out one step in finding the roots of an arbitrary quartic polynomial. Let $\Bbbk$ be a field of characteristic 0, let $\mathbb{K} = \Bbbk(p, q, r)$ be the field of fractions of the polynomial ring $\Bbbk[p, q, r]$ in n indeterminates, and let $\mathbb{L}$ be a splitting field of the polynomial

$$F(X) = X^4 + pX^2 + qX + r$$

in $\mathbb{K}[X]$. The Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is $\mathfrak{S}_4$ by the previous problem. Let $B_4 = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. In the composition series $\mathfrak{S}_4 \supseteq \mathfrak{A}_4 \supseteq B_4 \supseteq \{(1), (1\ 2)\}(3\ 4)\} \supseteq \{1\}$, Proposition 9.63 shows that the fixed field of $\mathfrak{A}_4$ is $\mathbb{K}(\sqrt{D})$, where D is the discriminant. To obtain the fixed field of B_4, we adjoin to $\mathbb{K}(\sqrt{D})$ an element of $\mathbb{L}$ invariant under B_4 but not under $\mathfrak{A}_4$. If s_1, s_2, s_3, s_4 denote the roots of $F(X)$ in $\mathbb{L}$, then such an element is $(s_1 + s_2)(s_3 + s_4)$. Its three conjugates under $\mathfrak{A}_4/B_4$ are

$$\begin{aligned}\theta_1 &= (s_1 + s_2)(s_3 + s_4),\\ \theta_2 &= (s_1 + s_3)(s_2 + s_4),\\ \theta_3 &= (s_1 + s_4)(s_2 + s_3),\end{aligned}$$

which are the three roots of the "cubic resolvent" polynomial

$$\theta^3 - c_1\theta^2 + c_2\theta - c_3,$$

where c_1, c_2, c_3 are the elementary symmetric polynomials in $\theta_1, \theta_2, \theta_3$ given by

$$c_1 = \sum_i \theta_i, \qquad c_2 = \sum_{i<j} \theta_i\theta_j, \qquad c_3 = \prod_i \theta_i.$$

(a) Show that c_1, c_2, c_3 are symmetric polynomials in s_1, s_2, s_3, s_4, hence are polynomials in the coefficients p, q, r.
(b) Verify that $c_1 = 2p$, $c_2 = p^2 - 4r$, and $c_3 = q^2$.
(c) Show that the discriminant of the cubic resolvent equals the discriminant of the original quartic polynomial.

Problems 46–50 concern Galois groups of splitting fields of quartic polynomials. Take as known that the discriminant of a quartic polynomial $F(X) = X^4 + pX^2 + qX + r$ is given by

$$-4p^3q^2 - 27q^4 + 16p^4r + 144pq^2r - 128p^2r^2 + 256r^3.$$

Let $\mathbb{K}$ be a splitting field for $F(X)$ over $\mathbb{Q}$, and let $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Regard G as a subgroup of the symmetric group $\mathfrak{S}_4$.

46. (a) Identify all transitive subgroups of the alternating group $\mathfrak{A}_4$, up to a relabeling of the four indices.
(b) Identify all transitive subgroups of the symmetric group $\mathfrak{S}_4$ other than those in (a), up to a relabeling of the four indices.

47. Suppose $q = 0$.
(a) Show that G is a subgroup of $\mathfrak{A}_4$ if and only if r is a square in $\mathbb{Q}$.
(b) Show by solving $F(X) = 0$ explicitly that $[\mathbb{K} : \mathbb{Q}]$ is a power of 2, and conclude that G has no element of order 3.
(c) Deduce when r is a square that $G = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ if $F(X)$ is irreducible over $\mathbb{Q}$.
(d) Deduce when r is a nonsquare that G is cyclic of order 4 or is dihedral of order 8 if $F(x)$ is irreducible over $\mathbb{Q}$; in the dihedral case, G is generated by a 4-cycle and the group listed in (c). (Problem 22 shows how to distinguish between the two cases.)

48. For $F(X) = X^4 + X + 1$, show by considering reduction modulo 2 and modulo 3 that $G = \mathfrak{S}_4$.

49. Let $F(X) = X^4 + 8X + 12$.
(a) Compute the discriminant of $F(X)$, and verify that it is a square.
(b) Show that $F(X) \equiv (1 + X)(2 + X + 4X^2 + X^3)$ mod 5 with the two factors on the right side irreducible in $\mathbb{F}_5$.
(c) Show from (a) and (b) that if $F(X)$ is reducible over $\mathbb{Q}$, then it must have a root that is an integer. Check that there is no such root.
(d) Conclude that $G = \mathfrak{A}_4$.

Pure Mathematical Physics

50. For each transitive group G as in Problem 46, find a polynomial $F(X)$ of degree 4 over $\mathbb{Q}$ whose splitting field $\mathbb{K}$ over $\mathbb{Q}$ has $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ isomorphic to G.

Problems 51–56 continue the introduction to error-correcting codes begun in Problems 63–73 at the end of Chapter IV and continued in Problems 25–28 at the end of Chapter VII. The current problems will not make use of the problems in Chapter VII. As in the problems in Chapter IV, we work with the field $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$, with Hamming space $\mathbb{F}^n$, and with linear codes C in $\mathbb{F}^n$. The minimal distance of C is denoted by $\delta(C)$. Problem 72 in Chapter IV introduced cyclic redundancy codes, which are determined by a generating polynomial $G(X)$ of some degree g suitably less than n. Such a code C is built from all polynomials $G(X)B(X)$ with $B(X) = 0$ or $\deg B(X) \le n - g - 1$. A given polynomial $c_0 + c_1X + \cdots$ becomes the n-tuple $(c_0, c_1, \dots)$ of C; the code C has dimension $n - g$. This set of problems will discuss a special class of cyclic redundancy codes called cyclic codes, and then a special subclass called BCH codes.

51. A linear code C in $\mathbb{F}^n$ is called a **cyclic code** if whenever $(c_0, c_1, \dots, c_{n-1})$ is in C, then so is $(c_{n-1}, c_0, c_1, \dots, c_{n-2})$.
    (a) Prove that a linear code C is cyclic if and only if the set of all polynomials $c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$ corresponding to members $(c_0, c_1, \dots, c_{n-1})$ of C is an ideal in the ring $\mathbb{F}[X]/(X^n - 1)$. (In this case the members of C will be identified with the set of such polynomials.)
    (b) Prove that if C is cyclic and nonzero, then there exists a unique $G(X)$ in C of lowest possible degree. Moreover, $G(X)$ divides $X^n - 1$ in $\mathbb{F}[X]$, and C consists exactly of the polynomials $G(X)F(X)$ mod $(X^n - 1)$ such that $F(X) = 0$ or $\deg F(X) \le n - \deg G(X) - 1$, and C has dimension $n - \deg G(X)$. (The polynomial $G(X)$ is called the **generating polynomial** of C. A cyclic code C over the field $\mathbb{Z}/2\mathbb{Z}$ having block length n and dimension k is called a **binary cyclic** (n, k) **code**.)
    (c) Prove that if $G(X)$ has degree $n - k$, then a basis of C consists of the polynomials $G(X), XG(X), X^2G(X), \dots, X^{k-1}G(X)$.
    (d) Under the assumption that C is cyclic and nonzero, (b) says that it is possible to write $X^n - 1 = G(X)H(X)$ for some $H(X)$ in $\mathbb{F}[X]$. Prove that a member $B(X)$ of $\mathbb{F}[X]/(X^n - 1)$ lies in C if and only if $H(X)B(X) \equiv 0 \bmod (X^n - 1)$.

52. (a) Show that the row space C of the matrix $\mathcal{G} = \begin{pmatrix} 1\,0\,0\,1\,0\,1\,1 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \end{pmatrix}$ is a cyclic $(7, 3)$ code with generating polynomial $G(X) = 1 + X^2 + X^3 + X^4$.
    (b) Show directly from $\mathcal{G}$ that C has minimal distance $\delta = 4$.
    (c) The polynomial $H(X) = 1 + X^2 + X^3$ has the property that $G(X)H(X) = X^7 - 1$ in $\mathbb{F}[X]$. Find a 4-by-7 matrix $\mathcal{H}$ such that the column vectors $v \in \mathbb{F}^7$ that lie in C are exactly the ones with $\mathcal{H}v = 0$.

Pure Mathematical Physics

(d) The matrix $\mathcal{H}$ in (c) is called the **check matrix** for the code. Describe a procedure for constructing the check matrix when starting from a general binary cyclic (n, k) code whose generating polynomial $G(X)$ is known and whose polynomial $H(X)$ with $G(X)H(X) = X^n - 1$ is known. Prove that the procedure works.

53. Show that $X^n - 1$ is a separable polynomial over $\mathbb{F}$ if n is odd but not if n is even.

54. Let C be a binary cyclic (n, k) code with generating polynomial $G(X)$, and suppose that n is odd. Let $\mathbb{K}$ be a finite extension field of $\mathbb{F}$ in which $X^n - 1$ splits, and let α be a primitive n^{th} root of 1, i.e., a root of $X^n - 1$ in $\mathbb{K}$ such that $\alpha^m \neq 1$ for $0 < m < n$. Suppose that r and s are integers with $0 \leq s < n$ and
$$G(\alpha^r) = G(\alpha^{r+1}) = \cdots = G(\alpha^{r+s}) = 0.$$
(a) Let $P(X) = G(X)F(X)$ with $F(X) \neq 0$ and $\deg F < k$ be an arbitrary nonzero member of C, so that $P(\alpha^r) = P(\alpha^{r+1}) = \cdots = P(\alpha^{r+s}) = 0$. Write $P(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$, and use the values of $P(\alpha^j)$ for $r \leq j \leq r + s$ to set up a homogeneous system of $s + 1$ linear equations with n unknowns $c_0, \ldots, c_{n-1}$.
(b) Using an argument with Vandermonde determinants, show that every $(s+1)$-by-$(s+1)$ submatrix of the coefficient matrix of the system in (a) is invertible.
(c) Obtain a contradiction from (b) if $s + 1$ or fewer of the coefficients of $P(X)$ are nonzero.
(d) Conclude that the minimal distance $\delta(C)$ is $\geq s + 2$.

55. **(BCH codes, or Bose–Chaudhuri–Hocquenghem codes)** Let n be an odd positive integer, let e be a positive integer $< n/2$, let $\mathbb{K}$ be a finite extension field of $\mathbb{F}$ in which $X^n - 1$ splits, and let α be a primitive n^{th} root of 1 in $\mathbb{K}$. For $1 \leq j \leq 2e$, let $F_j(X)$ be the minimal polynomial of α^j over $\mathbb{F}$, and define $G(X) = (1 + X)\,\mathrm{LCM}(F_1(X), \ldots, F_{2e}(X))$. Prove that $G(X)$ divides $X^n - 1$ and that $G(X)$ is the generating polynomial for a cyclic code C in $\mathbb{F}^n$ with minimal distance $\delta(C) \geq 2e + 2$. (Educational note: Therefore C has the built-in capability of correcting at least e errors.)

56. In the setting of the previous problem, let $n = 2^m - 1$ for a positive integer m, and let $\mathbb{K}$ be a field of order 2^m.
(a) Prove that any irreducible polynomial in $\mathbb{F}[X]$ with a root in $\mathbb{K}$ has order dividing m, and conclude that the order of the generating polynomial $G(X)$ in the previous problem is at most $2em + 1$.
(b) Prove that there exists a sequence C_r of binary cyclic (n_r, k_r) codes of BCH type such that k_r/n_r tends to 1 and the minimal distance $\delta(C_r)$ tends to infinity. (Educational note: The fraction k_r/n_r tells the fraction of message bits to total bits in each transmitted block. Thus the problem says that there are linear codes capable of correcting as large a number of errors as we please while having as large a percentage of message bits as we please.)

Pure Mathematical Physics

57. Take as known that $F_1(X) = 1 + X + X^4$ is irreducible over $\mathbb{F}$. Let $\mathbb{K}$ be the field $\mathbb{F}[X]/(F_1(X))$ of order 16, and let α be the coset $X + (F_1(X))$ in $\mathbb{K}$.
    (a) Explain why $F_1(X)$ factors as $F_1(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^4)(X-\alpha^8)$ over $\mathbb{K}$.
    (b) Find the minimal polynomial $F_3(X)$ of α^3.
    (c) Show in $\mathbb{F}^{15}$ that the binary cyclic code C with generating polynomial $G(X) = (1+X)F_1(X)F_3(X)$ has $\dim C = 6$ and $\delta(C) \geq 6$.

Problems 58-63 combine Problems 12–13 in Chapter V with the notion of extension of scalars from Chapter VI and some Galois theory from Chapter IX to prove the general **Jordan–Chevalley decomposition**. Let $\Bbbk$ be a field, and let V be a finite-dimensional vector space over $\Bbbk$. A linear map $N : V \to V$ is called **nilpotent** if $N^k = 0$ for some k. A linear map $S : V \to V$ is called **semisimple** if there is some finite extension $\mathbb{K}$ of $\Bbbk$ for which the linear map $S^{\mathbb{K}} : V^{\mathbb{K}} \to V^{\mathbb{K}}$ obtained by extension of scalars has a basis of eigenvectors. The theorem is that if $L : V \to V$ is a linear map with the property that every irreducible factor of the minimal polynomial of L over $\Bbbk$ is separable, then L has a unique decomposition $L = S + N$ with S semisimple, N nilpotent, and $SN = NS$. The theorem applies without restriction to a linear $L : V \to V$ if $\Bbbk$ is finite or has characteristic 0 because the separability condition is automatically satisfied in these cases.

58. Let $\Bbbk$ be a field, let V be a vector space over $\Bbbk$, and let $\mathbb{K}$ be an extension field of $\Bbbk$. Extend scalars to form the $\mathbb{K}$ vector space given by $V^{\mathbb{K}} = V \otimes_{\Bbbk} \mathbb{K}$, and let $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ act on $V^{\mathbb{K}}$ by saying that $\varphi(v \otimes c) = v \otimes \varphi(c)$ for φ in $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ and $v \otimes c$ in $V^{\mathbb{K}}$. Explain for $V = \Bbbk^n$ that $V^{\mathbb{K}}$ may be interpreted as $\mathbb{K}^n$ and that the action by φ reduces to $(\varphi(u))_j = \varphi(u_j)$.

59. Let $\Bbbk$ be a field, let V be a finite-dimensional vector space over $\Bbbk$, and let $L : V \to V$ be a linear map. Suppose that every irreducible factor of the minimal polynomial of L over $\Bbbk$ is separable. Prove the existence of a Jordan–Chevalley decomposition of L by following these steps:
    (a) Let $\mathbb{K}$ be a splitting field of $\Bbbk$, so that $\mathbb{K}$ is a finite Galois extension of $\Bbbk$. Use Problems 12–13 of Chapter V to show that $L \otimes 1 : V^{\mathbb{K}} \to V^{\mathbb{K}}$ has a unique decomposition as a sum $\mathcal{S} + \mathcal{N}$ of $\mathbb{K}$ linear maps of $V^{\mathbb{K}}$ to itself such that $\mathcal{S}\mathcal{N} = \mathcal{N}\mathcal{S}$, $\mathcal{N}$ is nilpotent, and $\mathcal{S}$ has a basis of eigenvectors.
    (b) Prove that any $\mathbb{K}$ linear $\mathcal{T} : V^{\mathbb{K}} \to V^{\mathbb{K}}$ such that $(1 \otimes \varphi)\mathcal{T} = \mathcal{T}(1 \otimes \varphi)$ for all $\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk)$ is of the form $\mathcal{T} = T \otimes 1$ for a unique $\Bbbk$ linear $T : V \to V$.
    (c) Show that the $\mathbb{K}$ linear maps $\mathcal{S}$ and $\mathcal{N}$ of (a) satisfy $(1 \otimes \varphi)\mathcal{S} = \mathcal{S}(1 \otimes \varphi)$ and $(1 \otimes \varphi)\mathcal{N} = \mathcal{N}(1 \otimes \varphi)$ for all $\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk)$, and deduce from (b) that $\mathcal{S}$ and $\mathcal{N}$ may be written as $\mathcal{S} = S \otimes 1$ and $\mathcal{N} = N \otimes 1$ for uniquely defined $\Bbbk$ linear maps S and N of V into itself.
    (d) Show that S is semisimple, N is nilpotent, and $SN = NS$, and conclude that $L = S + N$ is a Jordan–Chevalley decomposition of L.

Pure Mathematical Physics

(e) Show that S and N are polynomials in L.

60. Let $\Bbbk$ be a field, let V be a finite-dimensional vector space over $\Bbbk$, and let $L : V \to V$ be a linear map. Prove the uniqueness result that there is at most one decomposition $L = S + N$ with S semisimple, N nilpotent, and $SN = NS$.

61. Let $\Bbbk = \mathbb{R}$, and let $L : \mathbb{R}^4 \to \mathbb{R}^4$ be the linear map defined by the matrix

$$A = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

The minimal polynomial of L or A is $(X^2+1)^2$. Calculate the Jordan–Chevalley decomposition of L in matrix form.

62. Let $\mathbb{F}_2$ be a field of two elements, and let $\Bbbk = \mathbb{F}_2(x)$, where x is transcendental over $\mathbb{F}_2$. Let $L : \Bbbk^2 \to \Bbbk^2$ be the linear map defined by the matrix $A = \left(\begin{smallmatrix} 0 & x \\ 1 & 0 \end{smallmatrix}\right)$. The characteristic polynomial of L or A is $M(X) = X^2 - x$. This is irreducible over $\Bbbk$ and hence is also the minimal polynomial. The quadratic extension $\mathbb{K} = \Bbbk[x^{1/2}]$ of $\Bbbk$ is a splitting field for $M(X)$, and $M(X)$ has a double root in $\Bbbk[x^{1/2}]$.
   (a) Show that A, regarded as a matrix in $M_2(\mathbb{K})$, does not have a basis of eigenvectors. Conclude that L is not semisimple.
   (b) Calculate the most general 2-by-2 matrix commuting with A, and show that it cannot have characteristic polynomial X^2 unless it is the 0 matrix.
   (c) Conclude that L cannot have a Jordan–Chevalley decomposition.

63. Let $\Bbbk$ be a field, let V be a finite-dimensional vector space over $\Bbbk$, and let $L : V \to V$ be an *invertible* linear map. Suppose that every irreducible factor of the minimal polynomial of L over $\Bbbk$ is separable. A linear map $U : V \to V$ is called **unipotent** if $(U - I)^k = 0$ for some k. By suitably adjusting the proof of the Jordan–Chevalley decomposition, prove that there exist linear maps S and U of V into itself such that S is semisimple, U is unipotent, and $L = SU = US$.

Problems 64–73 introduce ordered fields, formally real fields, and real closed fields. An **ordered field** $\Bbbk$ is a field with a specified subset P of "positive" elements that is closed under addition and multiplication and is such that each nonzero element of $\Bbbk$ is in exactly one of P and $-P$. The fields $\mathbb{Q}$ and $\mathbb{R}$ are examples. A **formally real field** $\Bbbk$ is a field in which -1 is not the sum of squares. A **real closed field** $\Bbbk$ is a formally real field such that no proper algebraic extension of $\Bbbk$ is formally real. The problems together prove the existence part of the **Artin–Schreier Theorem**: If $\Bbbk$ is an ordered field with P as its set of positive elements and if $\overline{\Bbbk}$ is an algebraic closure, then there exists a real closed field $\mathbb{K}$ between $\Bbbk$ and $\overline{\Bbbk}$ that is an ordered field with P contained in its set of positive elements. Moreover, $\mathbb{K}$ is unique up to $\Bbbk$ isomorphism, and $\overline{\Bbbk}$ is of the form $\mathbb{K}(\sqrt{-1}\,)$.

Pure Mathematical Physics

64. Verify the following properties of an ordered field $\Bbbk$ when P is the set of positive elements:
    (a) 1 is in P,
    (b) every nonzero square is in P,
    (c) whenever a is in P, then so is a^{-1},
    (d) $\Bbbk$ is formally real,
    (e) $\Bbbk$ has characteristic 0.

65. In an ordered field $\Bbbk$ whose set of positive elements is P, define $x > y$ and $y < x$ to mean $x - y$ is in P. Let a, b, c, d be in $\Bbbk$. Check the following:
    (a) exactly one the relations $a > b$, $a = b$, and $a < b$ holds,
    (b) if $a > b$ and $b > c$, then $a > c$,
    (c) if $a > b$, then $a + c > b + c$,
    (d) if $a > b$ and $c > 0$, then $ac > bc$,
    (e) if $a > b > 0$, then $b^{-1} > a^{-1}$,
    (f) if $a > b > 0$ and $c > d > 0$, then $ac > bd$,
    (g) if $a > b$ and $c > d$, then $ac + bd > ad + bc$.

66. Let $\Bbbk$ be an ordered field with P as its set of positive elements, let $\Bbbk(x)$ be a transcendental extension, and define the positive elements of $\Bbbk(x)$ to be those for which the quotient of the leading coefficient of the numerator by the leading coefficient of the denominator is in P. Show that with this definition of the set of positive elements, $\Bbbk(x)$ becomes an ordered field in which $x > n$ for every positive integer n. (Then also $1/n > 1/x$ for every positive integer n by Problem 65e.)

67. (a) Show that $\mathbb{Q}(\sqrt{2}\,)$ becomes an ordered field in two distinct ways.
    (b) If $\Bbbk$ is an ordered field with P as its set of positive elements and if c is a member of P that is not a square, show that there are two ways of defining the set of positive elements P' of $\mathbb{K} = \Bbbk(\sqrt{c}\,)$ so that $\mathbb{K}$ becomes an ordered field with $P \subseteq P'$.

68. Let $\Bbbk$ be an ordered field, and let $\mathbb{K}$ be the extension that arises by adjoining the square roots of all the positive elements of $\mathbb{K}$. Prove that $\mathbb{K}$ is a formally real field by carrying out the following steps:
    (a) Show that if n is chosen as small as possible so that an equation $-1 = \sum_{j=1}^{k} p_j \xi_j^2$ holds in $\mathbb{K}$ with all p_j positive in $\Bbbk$ and all ξ_j in an extension $\Bbbk(\sqrt{c_1}\,, \dots, \sqrt{c_n}\,)$ of $\Bbbk$ with all c_j positive in $\Bbbk$, then writing
    $$\Bbbk(\sqrt{c_1}\,, \dots, \sqrt{c_n}\,) = \Bbbk(\sqrt{c_1}\,, \dots, \sqrt{c_{n-1}}\,)(\sqrt{c_n}\,)$$
    leads to an equation
    $$-1 = \sum_{j=1}^{k} p_j a_j^2 + \sum_{j=1}^{k} p_j c_n b_j^2 + 2\sqrt{c_n} \sum_{j=1}^{k} p_j a_j b_j \qquad (*)$$
    in which a_j and b_j are in $\Bbbk(\sqrt{c_1}\,, \dots, \sqrt{c_{n-1}}\,)$.

(b) Consider the third term on the right side of $(*)$, and show that a contradiction results if this term is 0 and a different contradiction arises if this term is not 0.

69. Let $\Bbbk$ be a formally real field, and let $\overline{\Bbbk}$ be an algebraic closure. Show that there exist maximal formally real subfields of $\overline{\Bbbk}$ containing $\Bbbk$, and show that any such is a real closed field.

70. Carry out the following steps to show that a real closed field $\Bbbk$ becomes an ordered field in one and only one way:
    (a) Suppose that $c \neq 0$ is not a square, hence that $\Bbbk(\sqrt{c}\,)$ is a quadratic extension of $\Bbbk$. Why is $-1 = \sum_{j=1}^{n} (a_j + b_j\sqrt{c}\,)^2$ for suitable members a_j and b_j of $\Bbbk$?
    (b) By expanding the identity in (a), show that c is not a sum of squares. In other words, every sum of squares in $\Bbbk$ is a square in $\Bbbk$.
    (c) Solve for c in the expansion in (b), and conclude that $-c$ is a square.
    (d) Conclude from the previous steps that the choice of P as the set of nonzero squares makes $\Bbbk$ into an ordered field and that there no other possible definition for the set P of positive elements that makes $\Bbbk$ into an ordered field.

71. Carry out the following steps to show that in any real closed field $\Bbbk$, every polynomial of odd degree has a root:
    (a) Show by induction that it is enough to handle irreducible polynomials of odd degree.
    (b) For an irreducible polynomial $Q(X)$ of odd degree n, let $\Bbbk(\alpha)$ be a simple algebraic extension of $\Bbbk$ such that $Q(\alpha) = 0$. Show that an expression of -1 as a sum of squares in $\Bbbk(\alpha)$ forces an identity $\sum_{j=1}^{k} R_j(X)^2 + Q(X)A(X) = -1$ for suitable polynomials $R_j(X)$ in $\Bbbk[X]$ of degree $\leq n-1$ and some polynomial $A(X)$ in $\Bbbk[X]$ of odd degree $\leq n-2$.
    (c) If r is a root of the polynomial $A(X)$ in (b), show that $\sum_{j=1}^{k} R_j(r)^2 = -1$, and deduce a contradiction.

72. By using the results of Problems 70–71 and taking into account the proof of Theorem 1.18 that appears in Section IX.10, prove that if $\Bbbk$ is a real closed field, then $\Bbbk(\sqrt{-1}\,)$ is algebraically closed.

73. Put the above results together to give a proof of the existence in the Artin–Schreier Theorem: if an ordered field $\Bbbk$ has P as its set of positive elements and $\overline{\Bbbk}$ as an algebraic closure, then there exists a real closed field $\mathbb{K}$ with $\Bbbk \subseteq \mathbb{K} \subset \overline{\Bbbk}$ such that $\overline{\Bbbk} = \mathbb{K}(\sqrt{-1}\,)$ and such that P is contained in the set of squares in $\overline{\Bbbk}$, i.e., such that the set of positive elements in the natural ordered-field structure on $\overline{\Bbbk}$ contains P.

Pure Mathematical Physics

The Algebra I Edition

BETTER Algebra FOR ALL